FIG. 1

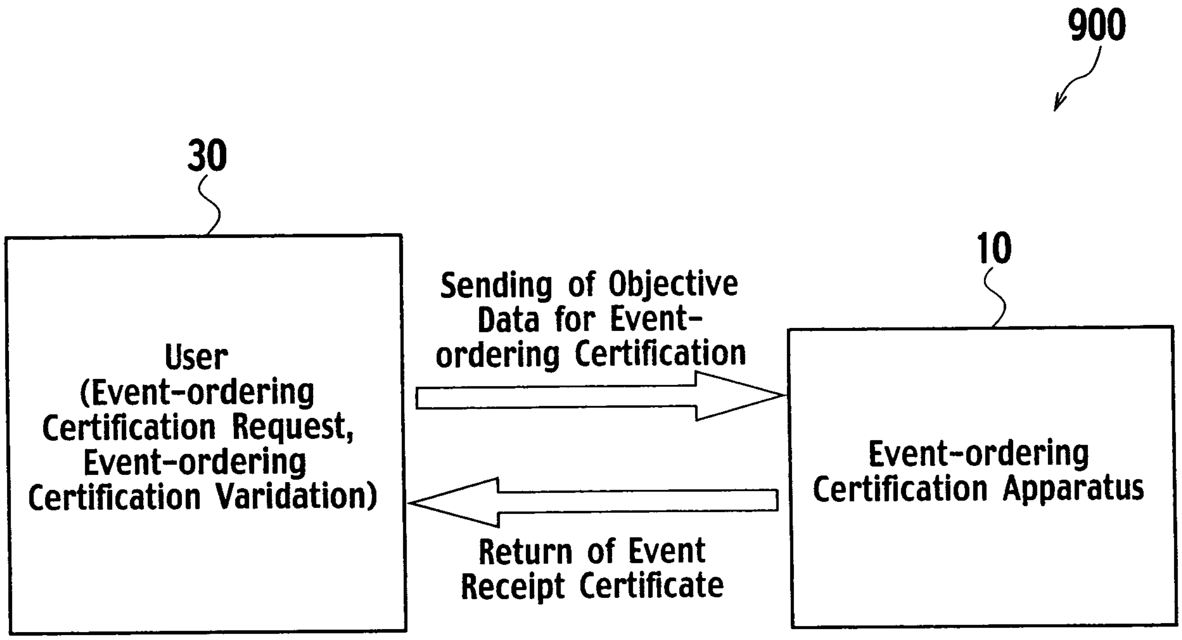

900
30
User
(Event-ordering
Certification Request,
Event-ordering
Certification Varidation)
Sending of Objective
Data for Event-
ordering Certification
10
Event-ordering
Certification Apparatus
Return of Event
Receipt Certificate

FIG. 2

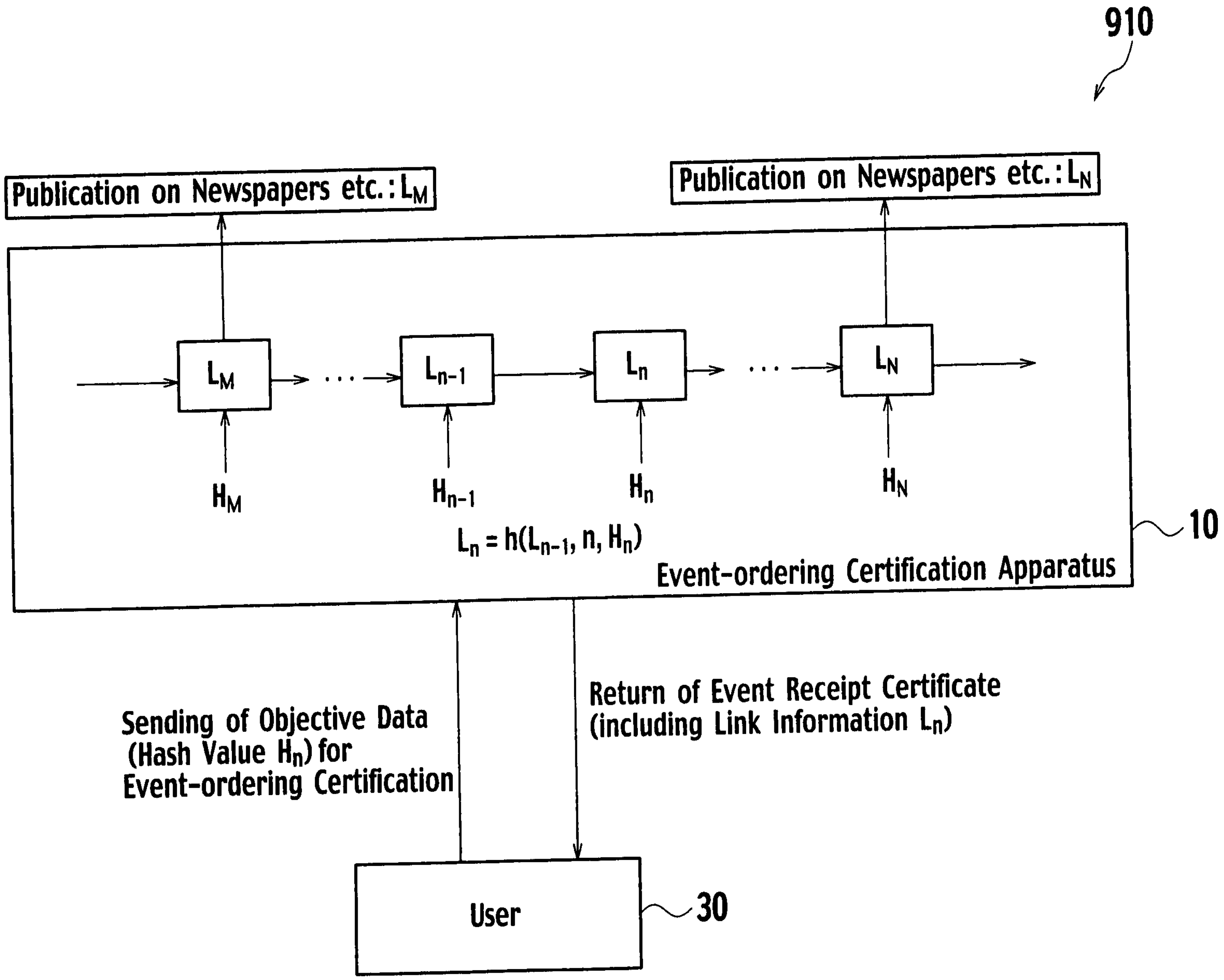

910
Publication on Newspapers etc.: L_M
Publication on Newspapers etc.: L_N
L_M
L_{n-1}
L_n
L_N
H_M
H_{n-1}
H_n
H_N
$L_n = h(L_{n-1}, n, H_n)$
Event-ordering Certification Apparatus
10
Sending of Objective Data (Hash Value H_n) for Event-ordering Certification
Return of Event Receipt Certificate (including Link Information L_n)
User
30

FIG. 3

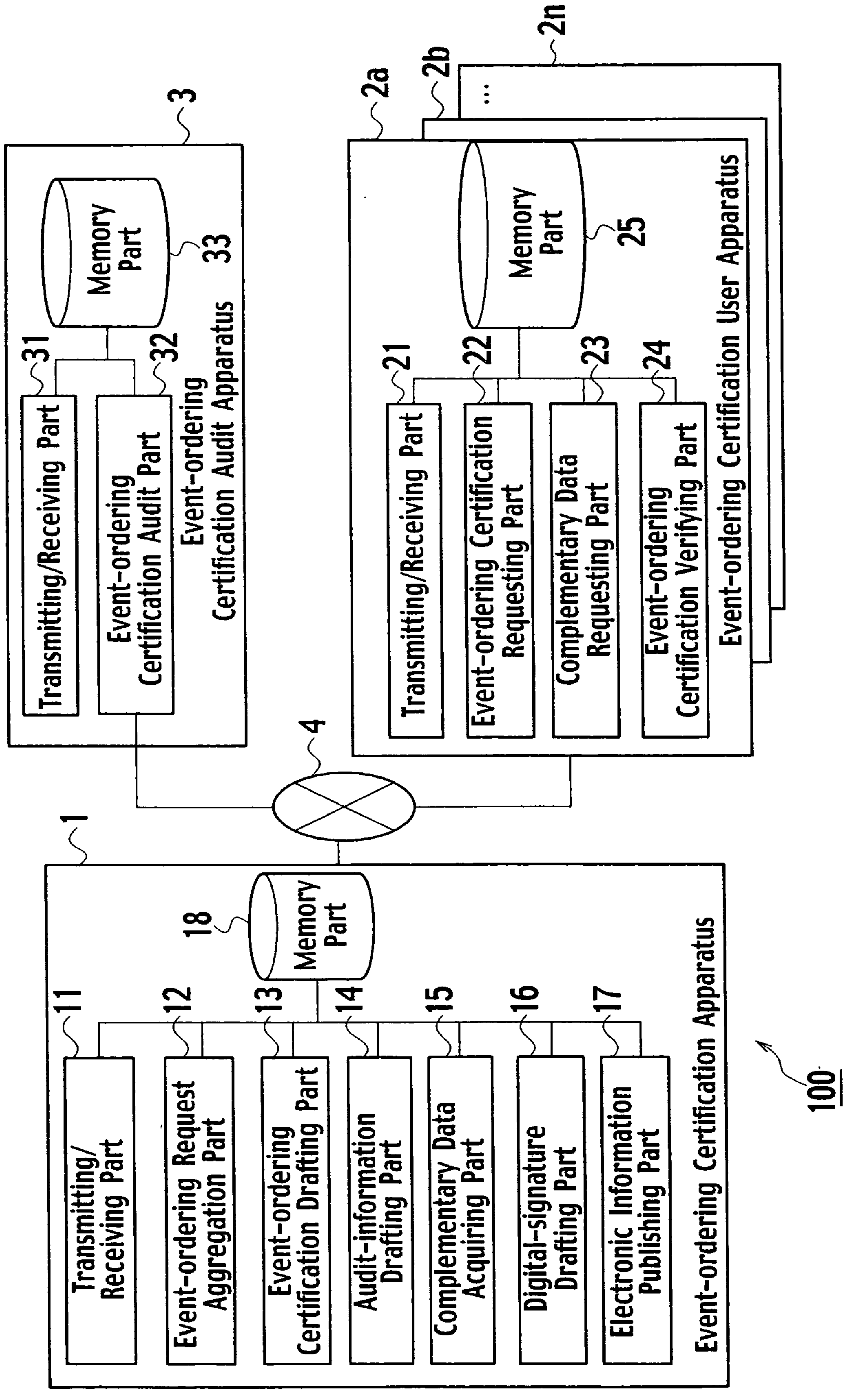

3
Transmitting/Receiving Part
31
Event-ordering Certification Audit Part
32
Memory Part
33
Event-ordering Certification Audit Apparatus
2a
2b
2n
...
Transmitting/Receiving Part
21
Event-ordering Certification Requesting Part
22
Complementary Data Requesting Part
23
Event-ordering Certification Verifying Part
24
Memory Part
25
Event-ordering Certification User Apparatus
4
1
Transmitting/Receiving Part
11
Event-ordering Request Aggregation Part
12
Event-ordering Certification Drafting Part
13
Audit-information Drafting Part
14
Complementary Data Acquiring Part
15
Digital-signature Drafting Part
16
Electronic Information Publishing Part
17
Memory Part
18
Event-ordering Certification Apparatus
100

FIG. 4

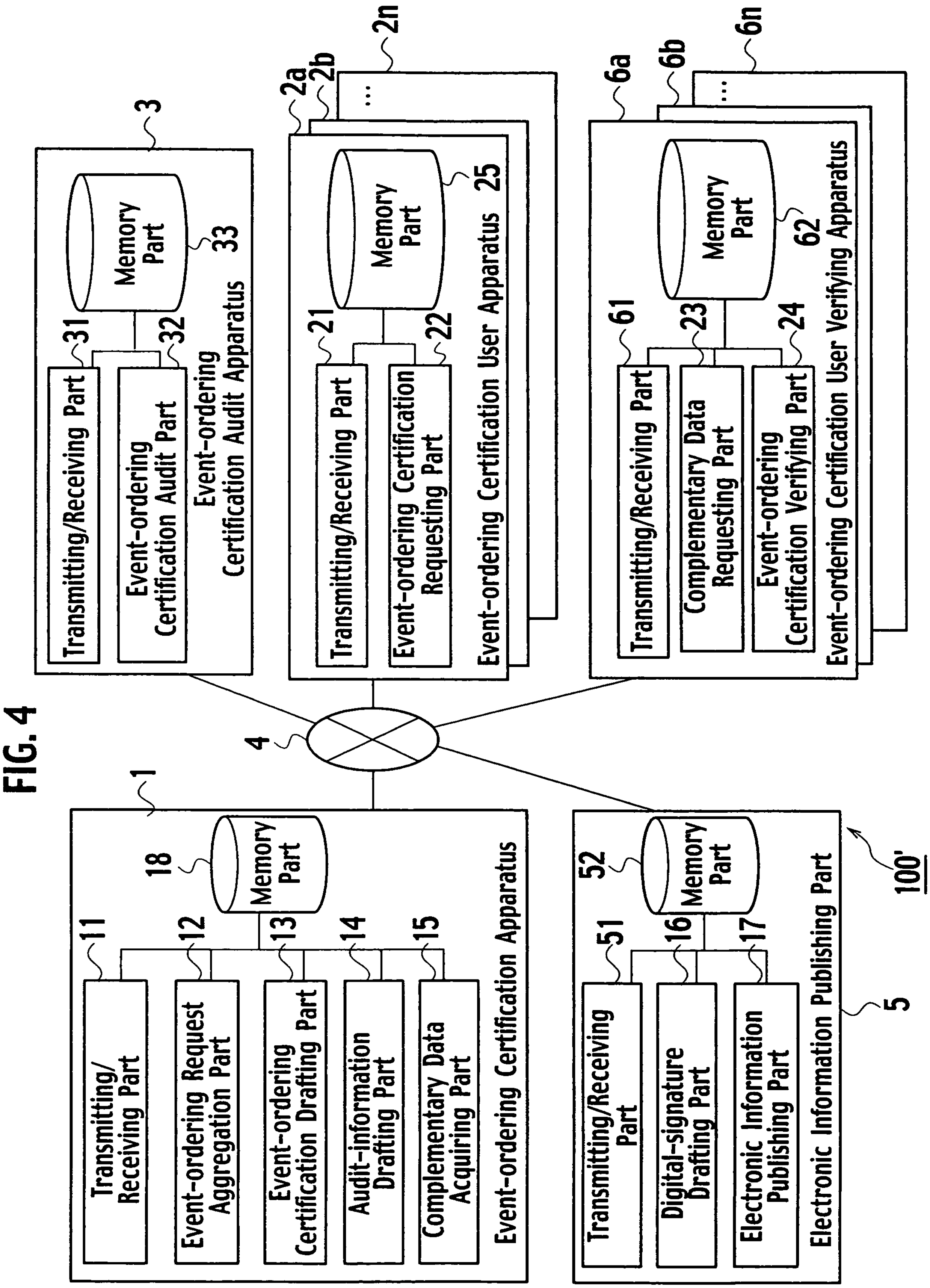

1
Transmitting/Receiving Part
11
Event-ordering Request Aggregation Part
12
Event-ordering Certification Drafting Part
13
Audit-information Drafting Part
14
Complementary Data Acquiring Part
15
Memory Part
18
Event-ordering Certification Apparatus
4
3
Transmitting/Receiving Part
31
Event-ordering Certification Audit Part
32
Memory Part
33
Event-ordering Certification Audit Apparatus
2a
2b
2n
...
Transmitting/Receiving Part
21
Event-ordering Certification Requesting Part
22
Memory Part
25
Event-ordering Certification User Apparatus
6a
6b
6n
...
Transmitting/Receiving Part
61
Complementary Data Requesting Part
23
Event-ordering Certification Verifying Part
24
Memory Part
62
Event-ordering Certification User Verifying Apparatus
Transmitting/Receiving Part
51
Digital-signature Drafting Part
16
Electronic Information Publishing Part
17
Memory Part
52
Electronic Information Publishing Part
5
100'

FIG. 5

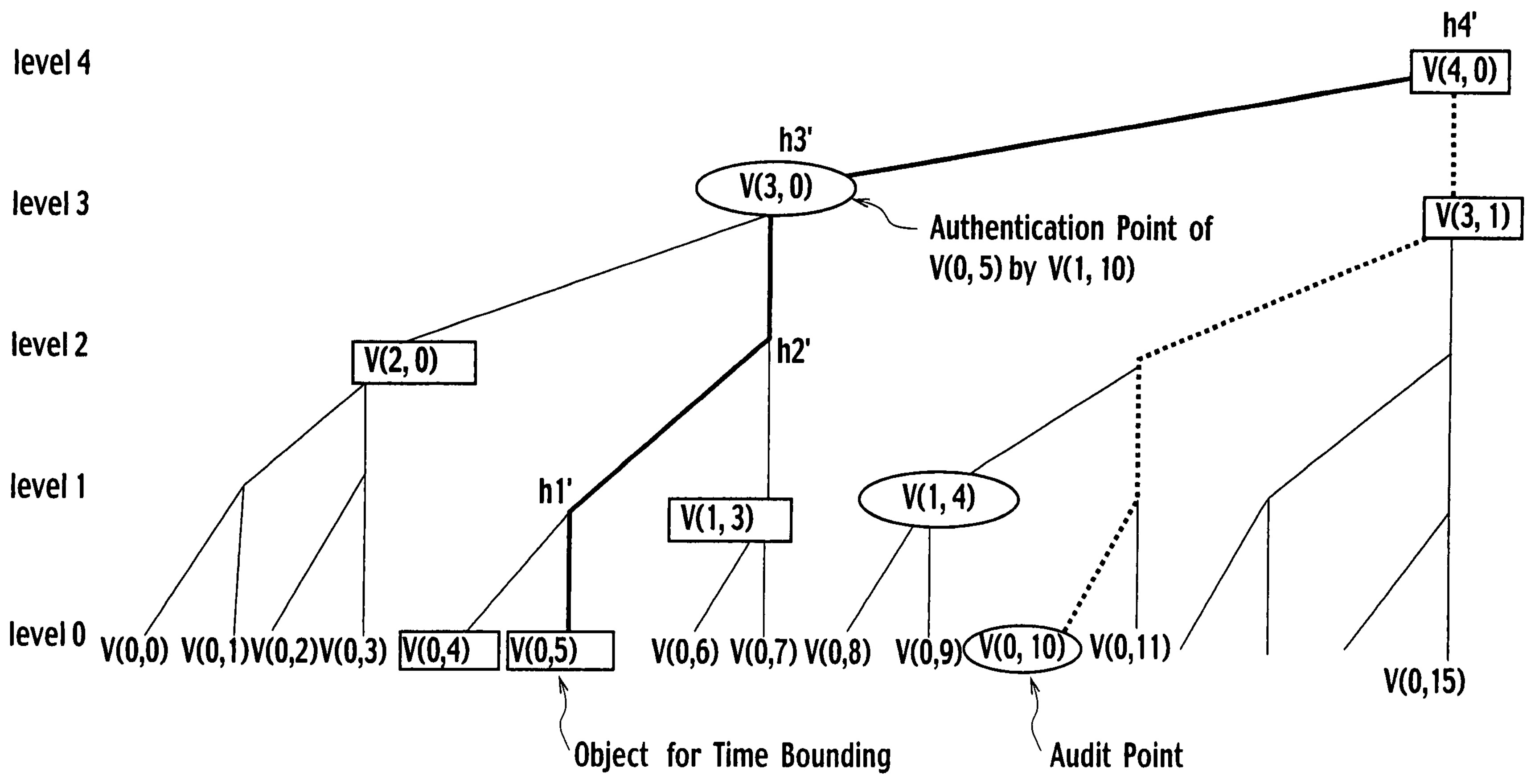

h4'
level 4
V(4, 0)
h3'
level 3
V(3, 0)
Authentication Point of
V(0, 5) by V(1, 10)
V(3, 1)
level 2
V(2, 0)
h2'
level 1
h1'
V(1, 3)
V(1, 4)
level 0
V(0,0)
V(0,1)
V(0,2)
V(0,3)
V(0,4)
V(0,5)
V(0,6)
V(0,7)
V(0,8)
V(0,9)
V(0, 10)
V(0,11)
V(0,15)
Object for Time Bounding
Audit Point

FIG. 6

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data (Positional Info. Assigned Value)	HK	
Digital Signature	DS	

FIG. 7

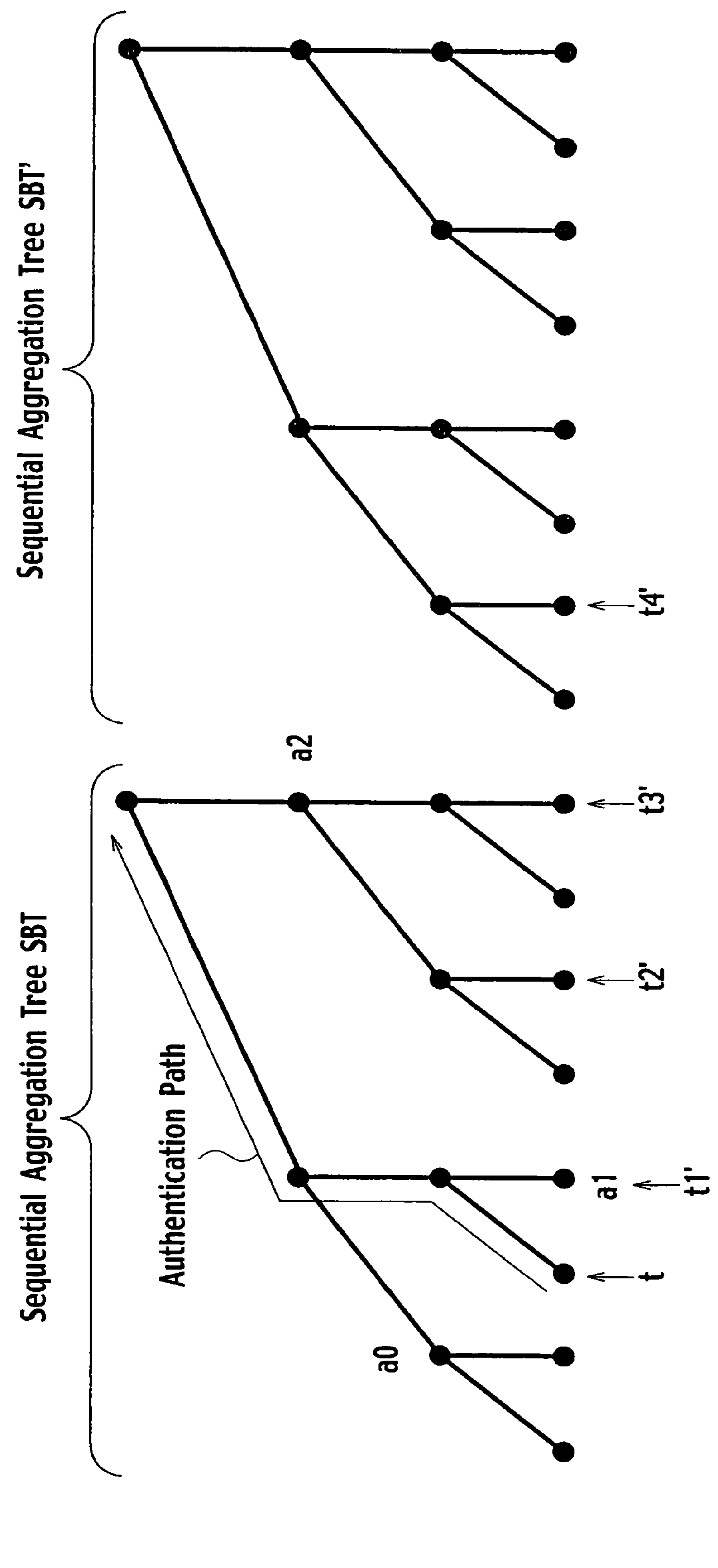

Sequential Aggregation Tree SBT'
t4'
a2
t3'
t2'
Sequential Aggregation Tree SBT
Authentication Path
a1
t1'
t
a0

FIG. 8

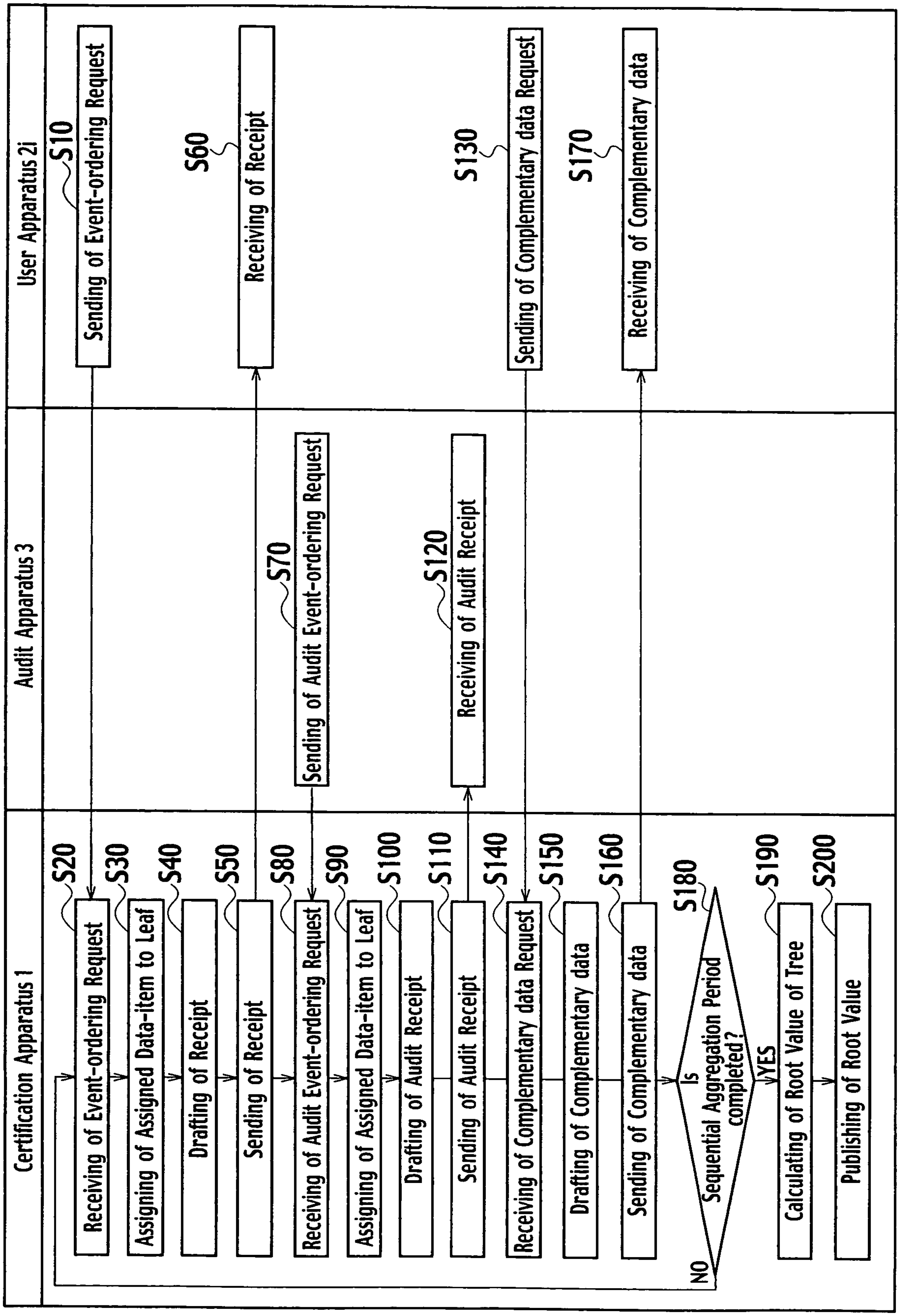
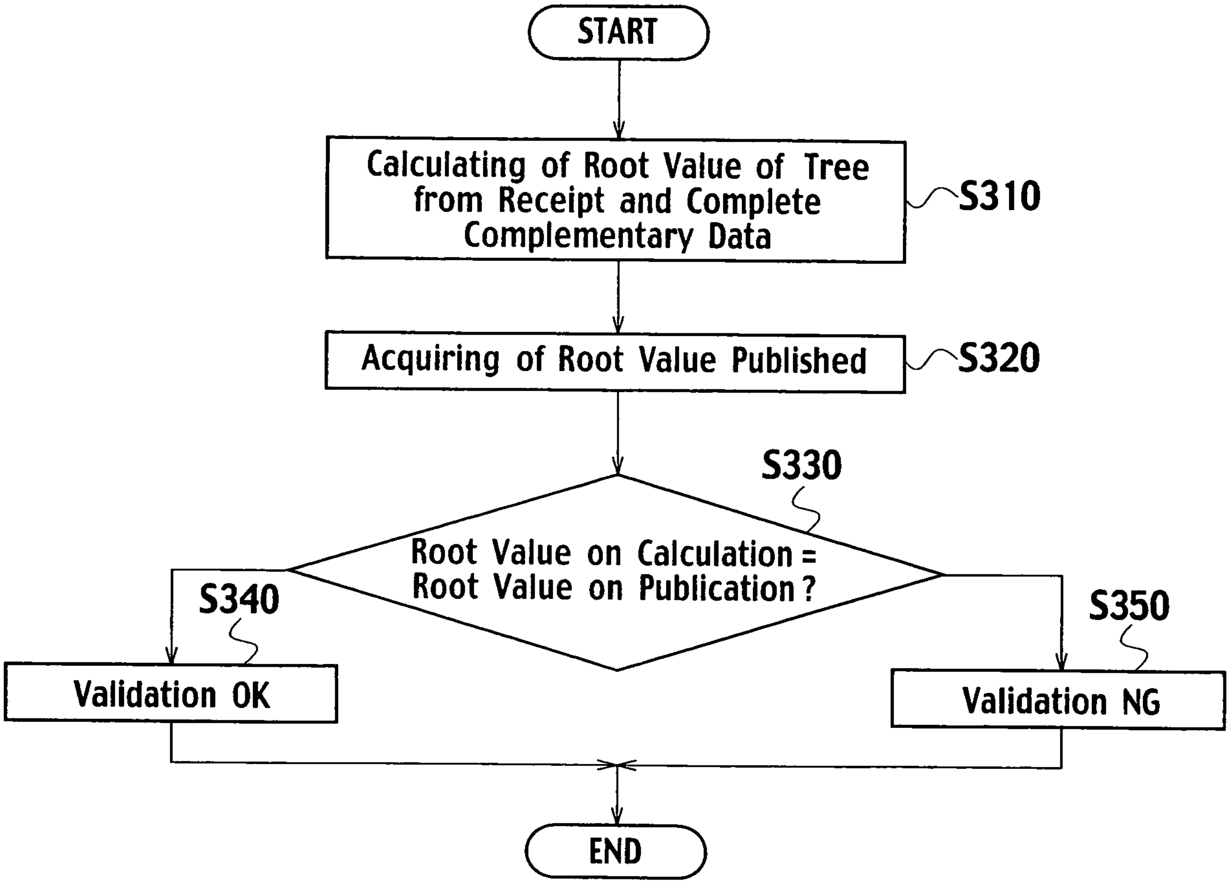

Certification Apparatus 1
Audit Apparatus 3
User Apparatus 2i
S10
Sending of Event-ordering Request
S20
Receiving of Event-ordering Request
S30
Assigning of Assigned Data-item to Leaf
S40
Drafting of Receipt
S50
Sending of Receipt
S60
Receiving of Receipt
S70
Sending of Audit Event-ordering Request
S80
Receiving of Audit Event-ordering Request
S90
Assigning of Assigned Data-item to Leaf
S100
Drafting of Audit Receipt
S110
Sending of Audit Receipt
S120
Receiving of Audit Receipt
S130
Sending of Complementary data Request
S140
Receiving of Complementary data Request
S150
Drafting of Complementary data
S160
Sending of Complementary data
S170
Receiving of Complementary data
S180
Is Sequential Aggregation Period completed?
YES
NO
S190
Calculating of Root Value of Tree
S200
Publishing of Root Value

FIG. 9


START
Calculating of Root Value of Tree from Receipt and Complete Complementary Data
S310
Acquiring of Root Value Published
S320
S330
Root Value on Calculation = Root Value on Publication ?
S340
Validation OK
S350
Validation NG
END

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 10 of 77

FIG. 10

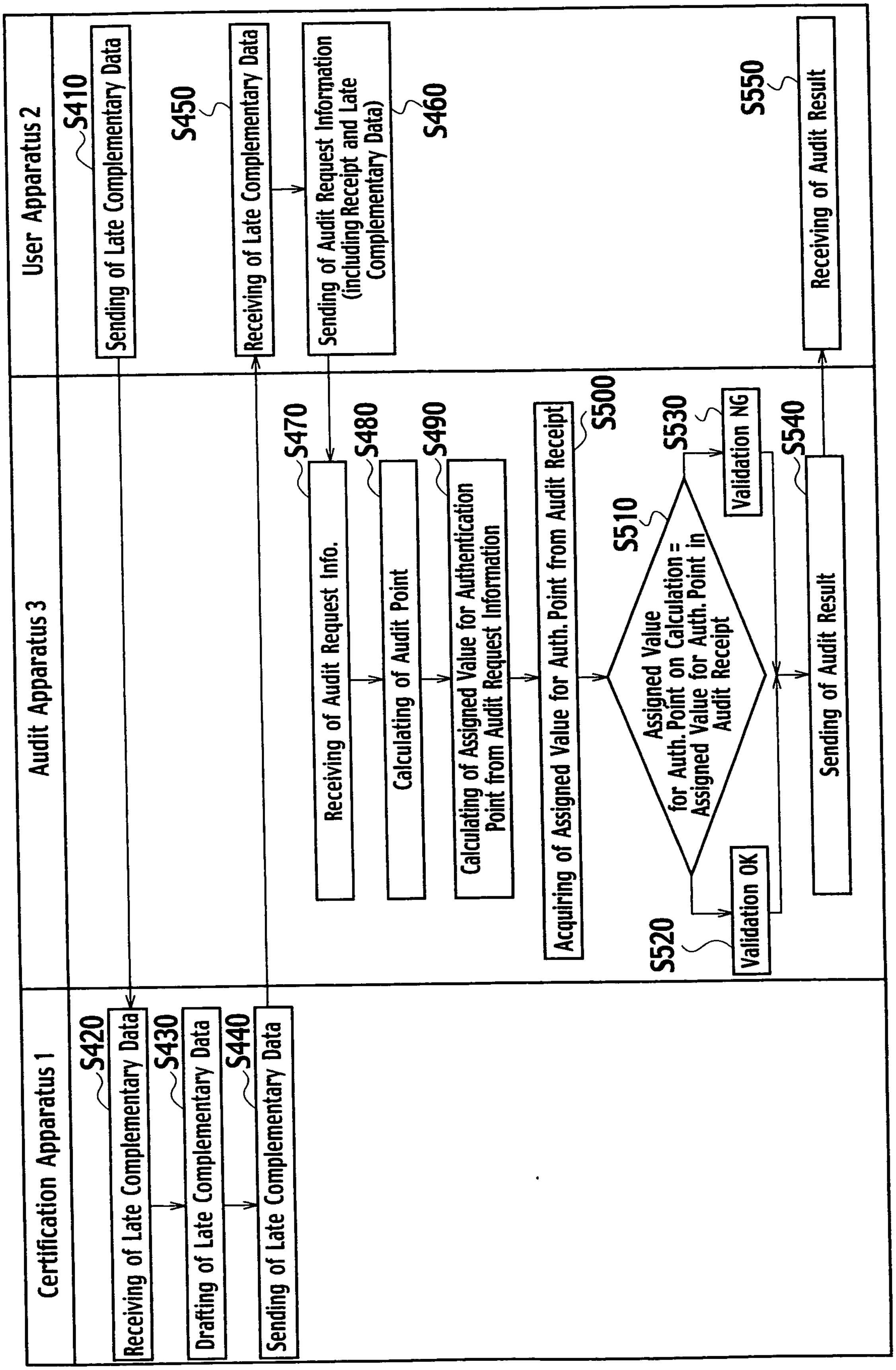

Certification Apparatus 1
Audit Apparatus 3
User Apparatus 2
S410
Sending of Late Complementary Data
S420
Receiving of Late Complementary Data
S430
Drafting of Late Complementary Data
S440
Sending of Late Complementary Data
S450
Receiving of Late Complementary Data
S460
Sending of Audit Request Information (including Receipt and Late Complementary Data)
S470
Receiving of Audit Request Info.
S480
Calculating of Audit Point
S490
Calculating of Assigned Value for Authentication Point from Audit Request Information
S500
Acquiring of Assigned Value for Auth. Point from Audit Receipt
S510
Assigned Value for Auth. Point on Calculation = Assigned Value for Auth. Point in Audit Receipt
S520
Validation OK
S530
Validation NG
S540
Sending of Audit Result
S550
Receiving of Audit Result

FIG. 11

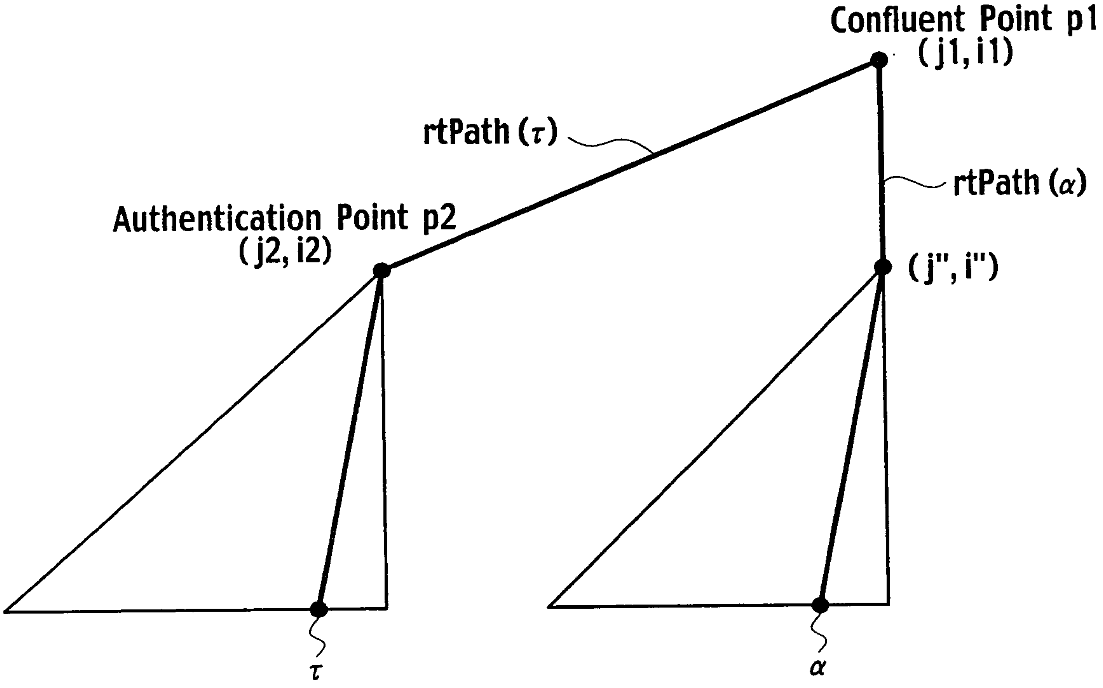
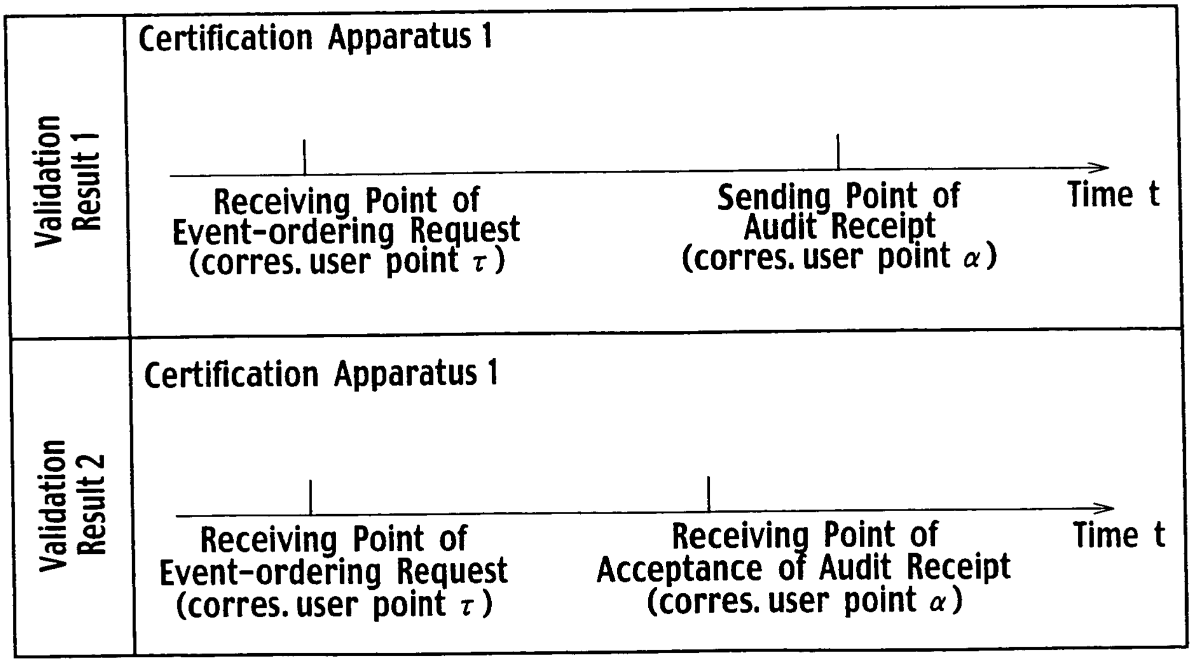

Confluent Point p1
(j1, i1)
rtPath (τ)
rtPath (α)
Authentication Point p2
(j2, i2)
(j", i")
τ
α

FIG. 12


Validation Result 1
Certification Apparatus 1
Receiving Point of Event-ordering Request (corres. user point τ)
Sending Point of Audit Receipt (corres. user point α)
Time t
Validation Result 2
Certification Apparatus 1
Receiving Point of Event-ordering Request (corres. user point τ)
Receiving Point of Acceptance of Audit Receipt (corres. user point α)
Time t

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 12 of 77

FIG. 13

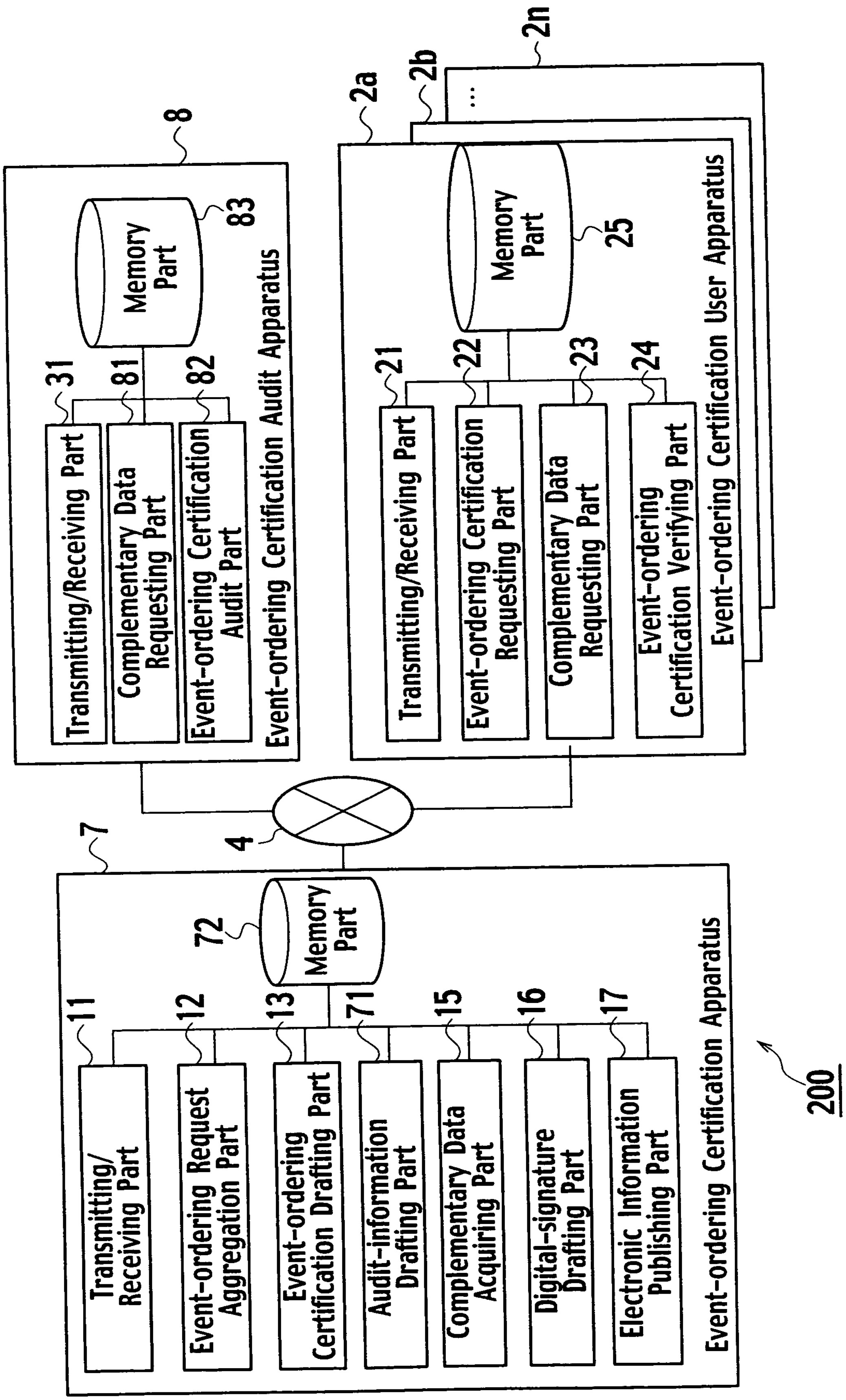
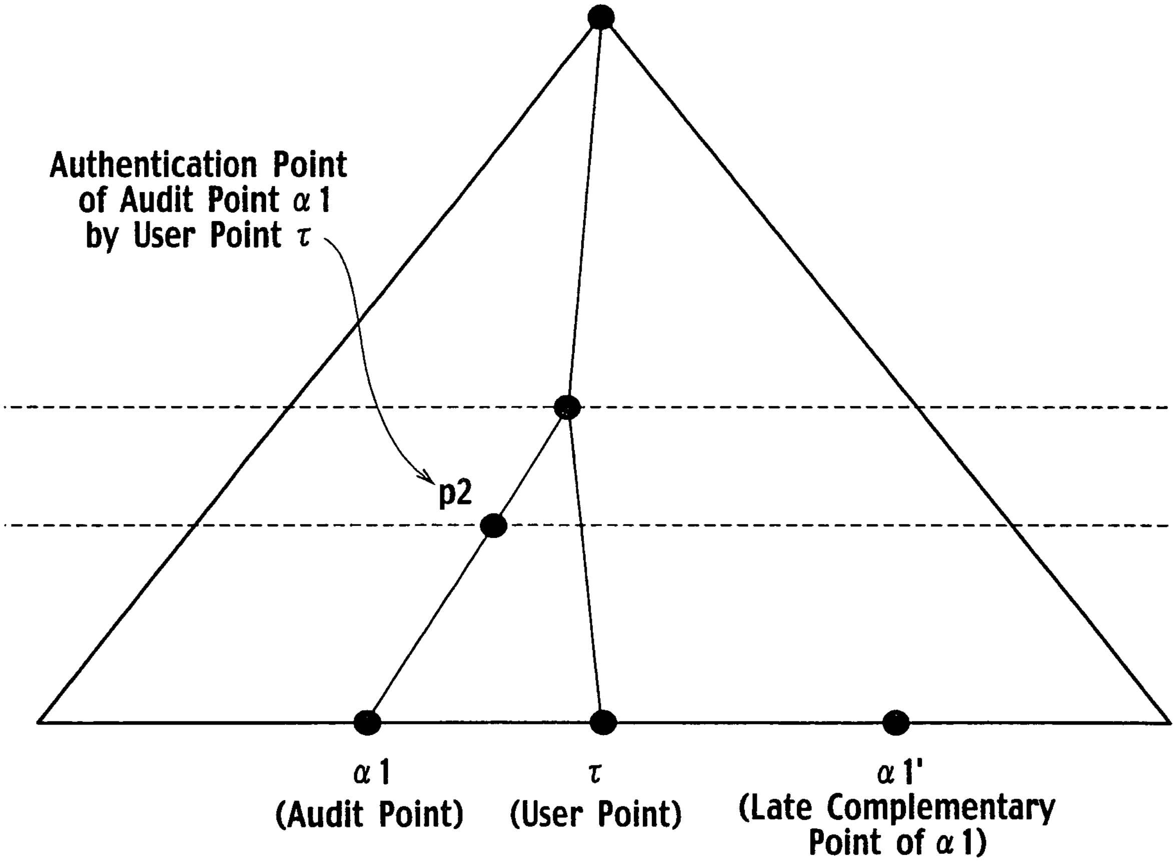

8
Memory Part
83
31
81
82
Transmitting/Receiving Part
Complementary Data Requesting Part
Event-ordering Certification Audit Part
Event-ordering Certification Audit Apparatus
2a
2b
2n
...
Memory Part
25
21
22
23
24
Transmitting/Receiving Part
Event-ordering Certification Requesting Part
Complementary Data Requesting Part
Event-ordering Certification Verifying Part
Event-ordering Certification User Apparatus
4
7
Memory Part
72
11
12
13
71
15
16
17
Transmitting/ Receiving Part
Event-ordering Request Aggregation Part
Event-ordering Certification Drafting Part
Audit-information Drafting Part
Complementary Data Acquiring Part
Digital-signature Drafting Part
Electronic Information Publishing Part
Event-ordering Certification Apparatus
200

FIG. 14


Authentication Point
of Audit Point α1
by User Point τ
p2
α1
(Audit Point)
τ
(User Point)
α1'
(Late Complementary
Point of α1)

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 14 of 77

FIG. 15

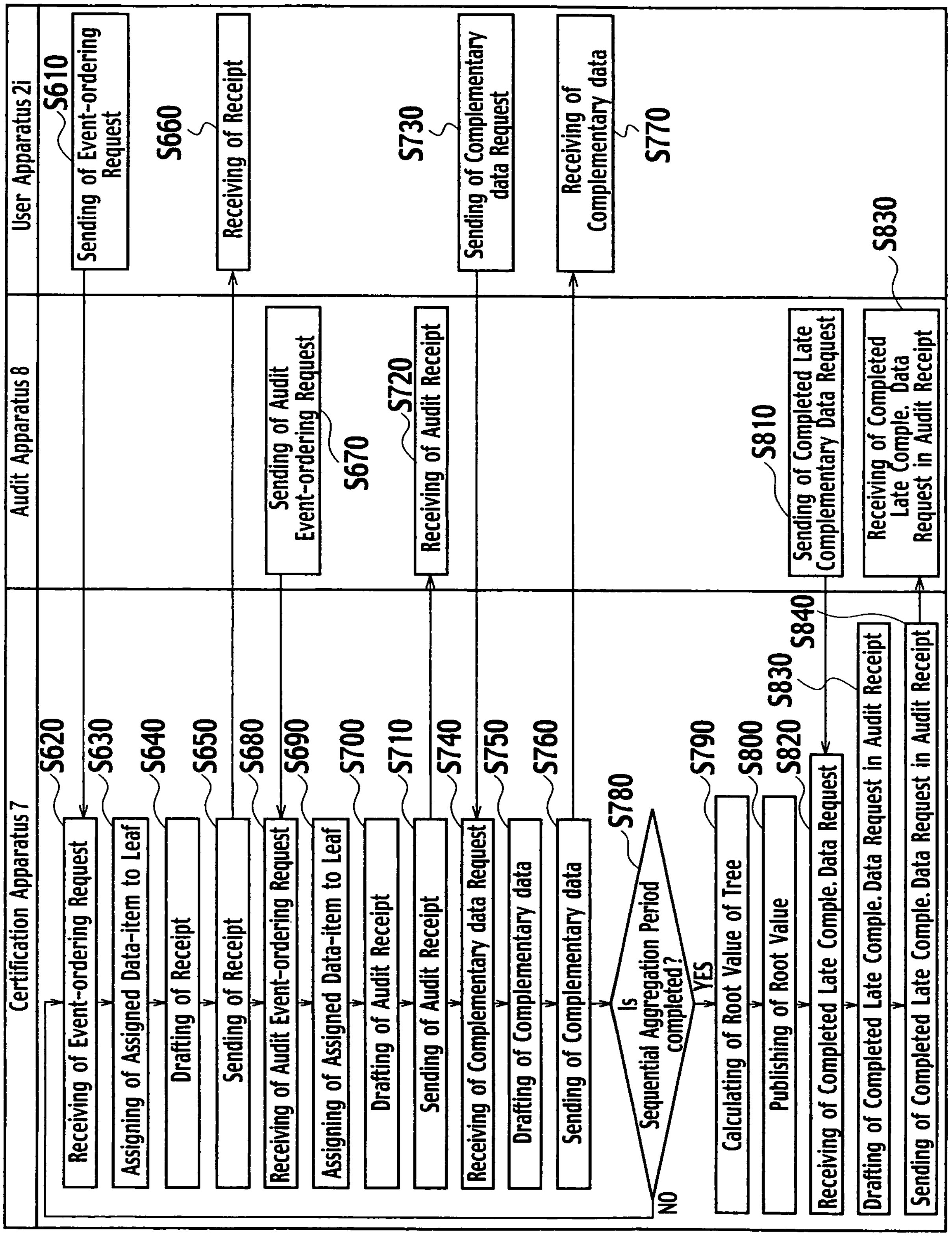

Certification Apparatus 7
Audit Apparatus 8
User Apparatus 2i
S610
Sending of Event-ordering Request
S620
Receiving of Event-ordering Request
S630
Assigning of Assigned Data-item to Leaf
S640
Drafting of Receipt
S650
Sending of Receipt
S660
Receiving of Receipt
S670
Sending of Audit Event-ordering Request
S680
Receiving of Audit Event-ordering Request
S690
Assigning of Assigned Data-item to Leaf
S700
Drafting of Audit Receipt
S710
Sending of Audit Receipt
S720
Receiving of Audit Receipt
S730
Sending of Complementary data Request
S740
Receiving of Complementary data Request
S750
Drafting of Complementary data
S760
Sending of Complementary data
S770
Receiving of Complementary data
S780
Is Sequential Aggregation Period completed?
YES
NO
S790
Calculating of Root Value of Tree
S800
Publishing of Root Value
S810
Sending of Completed Late Complementary Data Request
S820
Receiving of Completed Late Comple. Data Request
S830
Drafting of Completed Late Comple. Data Request in Audit Receipt
S840
Sending of Completed Late Comple. Data Request in Audit Receipt
S830
Receiving of Completed Late Comple. Data Request in Audit Receipt

FIG. 16

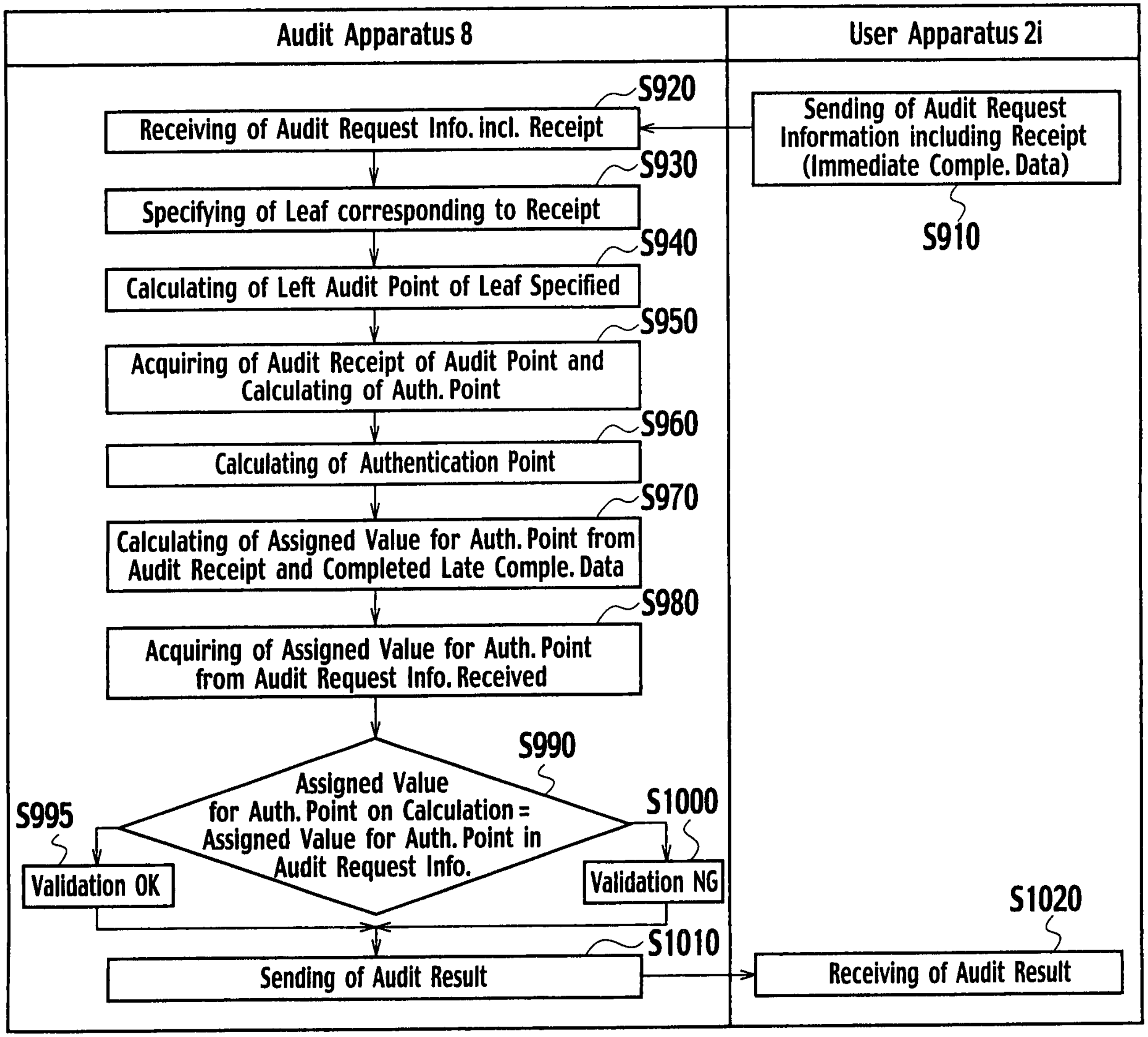

Audit Apparatus 8
User Apparatus 2i
Sending of Audit Request Information including Receipt (Immediate Comple. Data)
S910
S920
Receiving of Audit Request Info. incl. Receipt
S930
Specifying of Leaf corresponding to Receipt
S940
Calculating of Left Audit Point of Leaf Specified
S950
Acquiring of Audit Receipt of Audit Point and Calculating of Auth. Point
S960
Calculating of Authentication Point
S970
Calculating of Assigned Value for Auth. Point from Audit Receipt and Completed Late Comple. Data
S980
Acquiring of Assigned Value for Auth. Point from Audit Request Info. Received
S990
Assigned Value for Auth. Point on Calculation = Assigned Value for Auth. Point in Audit Request Info.
S995
Validation OK
S1000
Validation NG
S1010
Sending of Audit Result
S1020
Receiving of Audit Result

FIG. 17

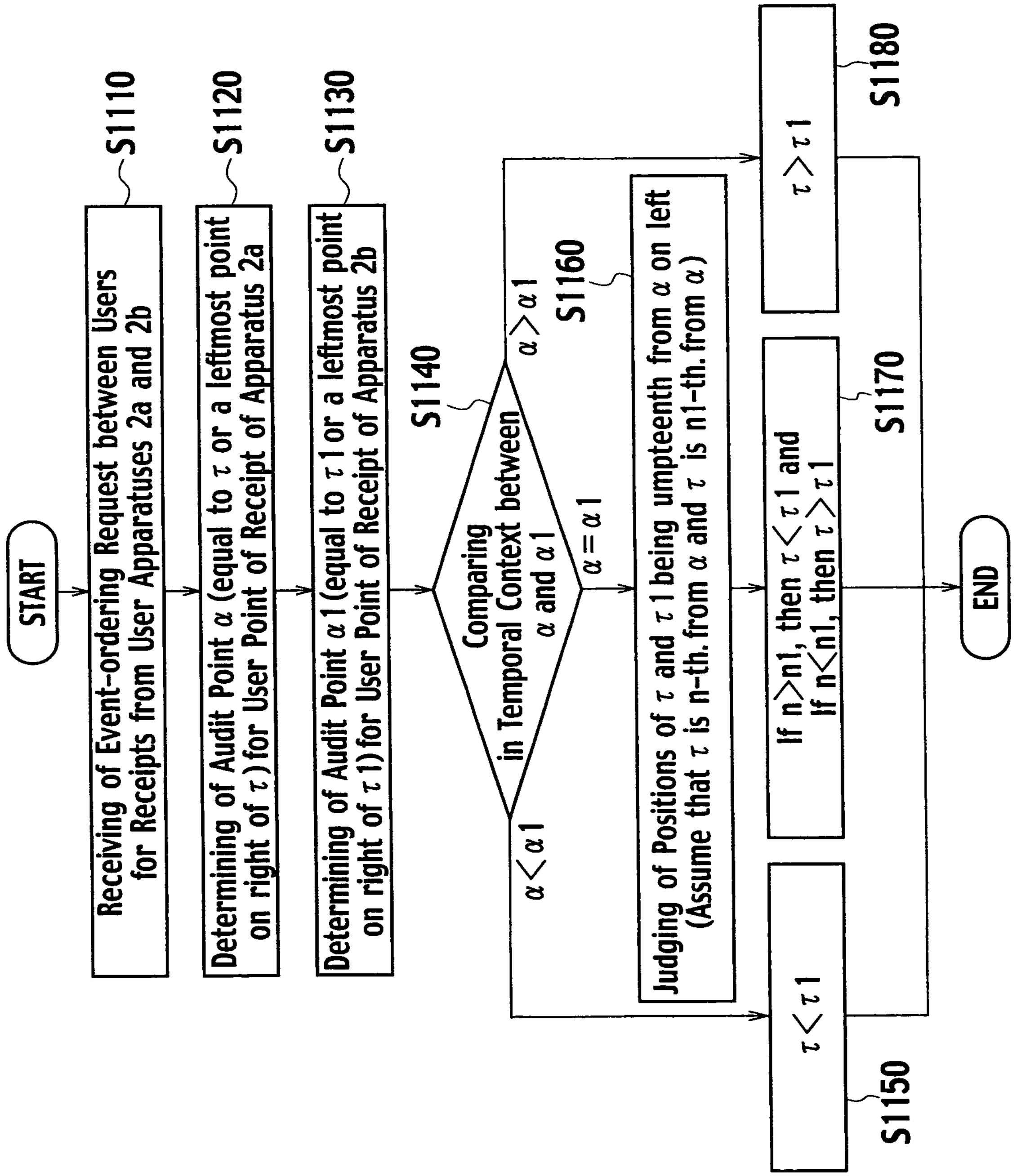

START
Receiving of Event-ordering Request between Users for Receipts from User Apparatuses 2a and 2b
S1110
Determining of Audit Point α (equal to τ or a leftmost point on right of τ) for User Point of Receipt of Apparatus 2a
S1120
Determining of Audit Point α1 (equal to τ1 or a leftmost point on right of τ1) for User Point of Receipt of Apparatus 2b
S1130
Comparing in Temporal Context between α and α1
S1140
α<α1
α=α1
α>α1
Judging of Positions of τ and τ1 being umpteenth from α on left (Assume that τ is n-th. from α and τ is n1-th. from α)
S1160
τ<τ1
S1150
If n>n1, then τ<τ1 and If n<n1, then τ>τ1
S1170
τ>τ1
S1180
END

FIG. 18

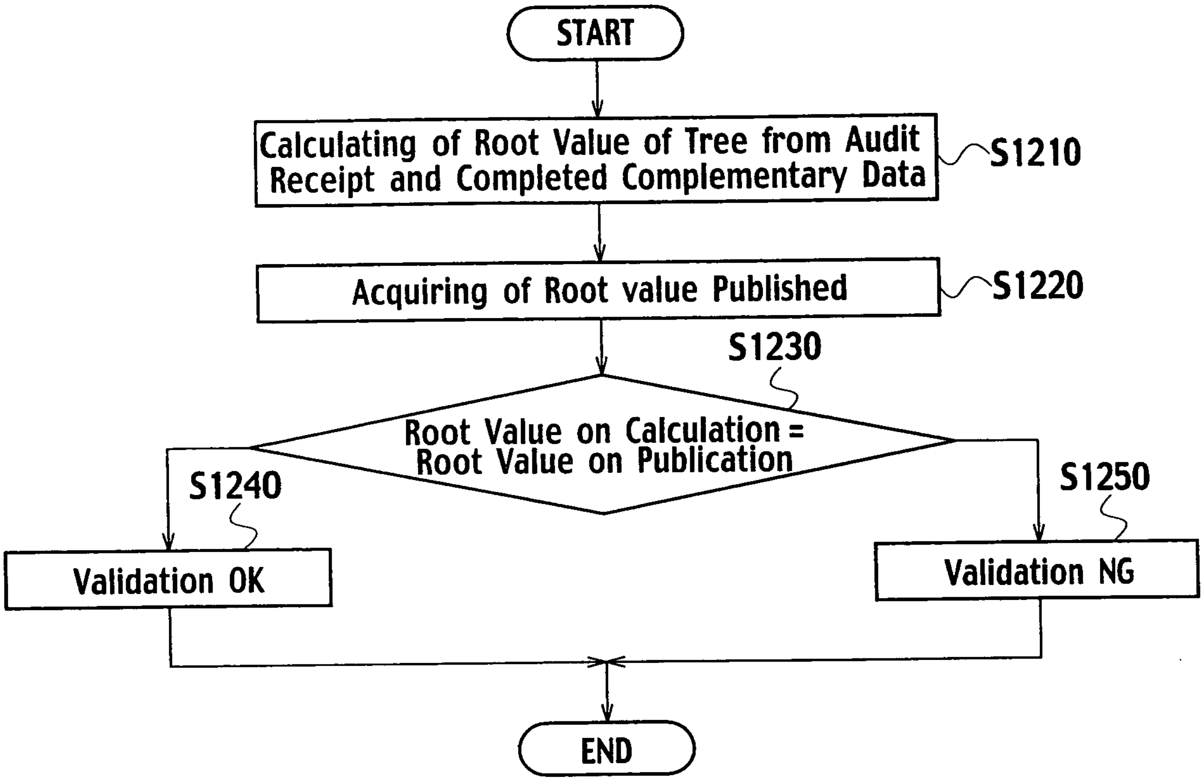

START
Calculating of Root Value of Tree from Audit Receipt and Completed Complementary Data
S1210
Acquiring of Root value Published
S1220
S1230
Root Value on Calculation = Root Value on Publication
S1240
S1250
Validation OK
Validation NG
END

FIG. 19

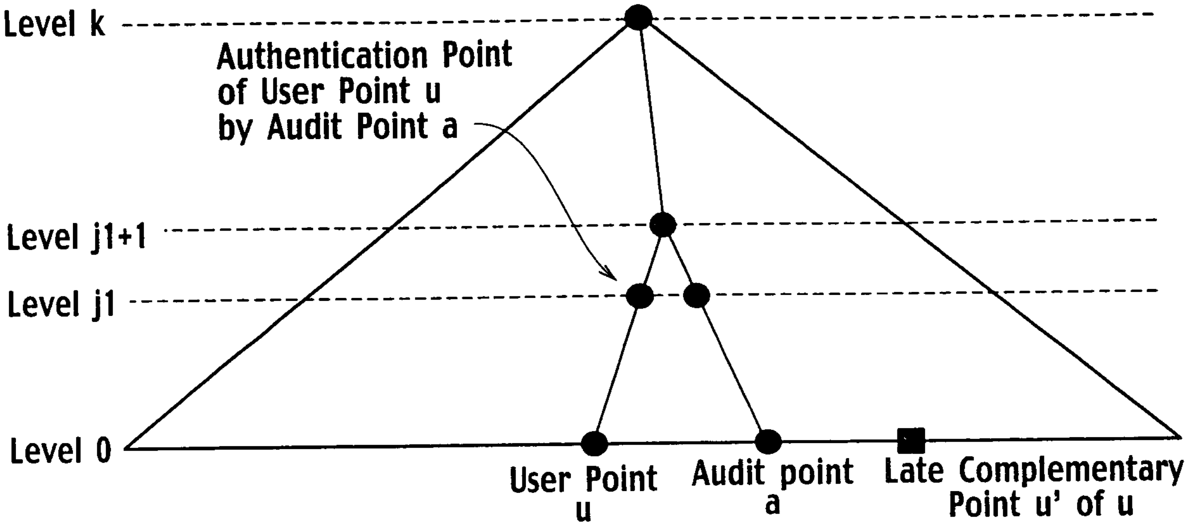

Level k
Authentication Point of User Point u by Audit Point a
Level j1+1
Level j1
Level 0
User Point u
Audit point a
Late Complementary Point u' of u

FIG. 20

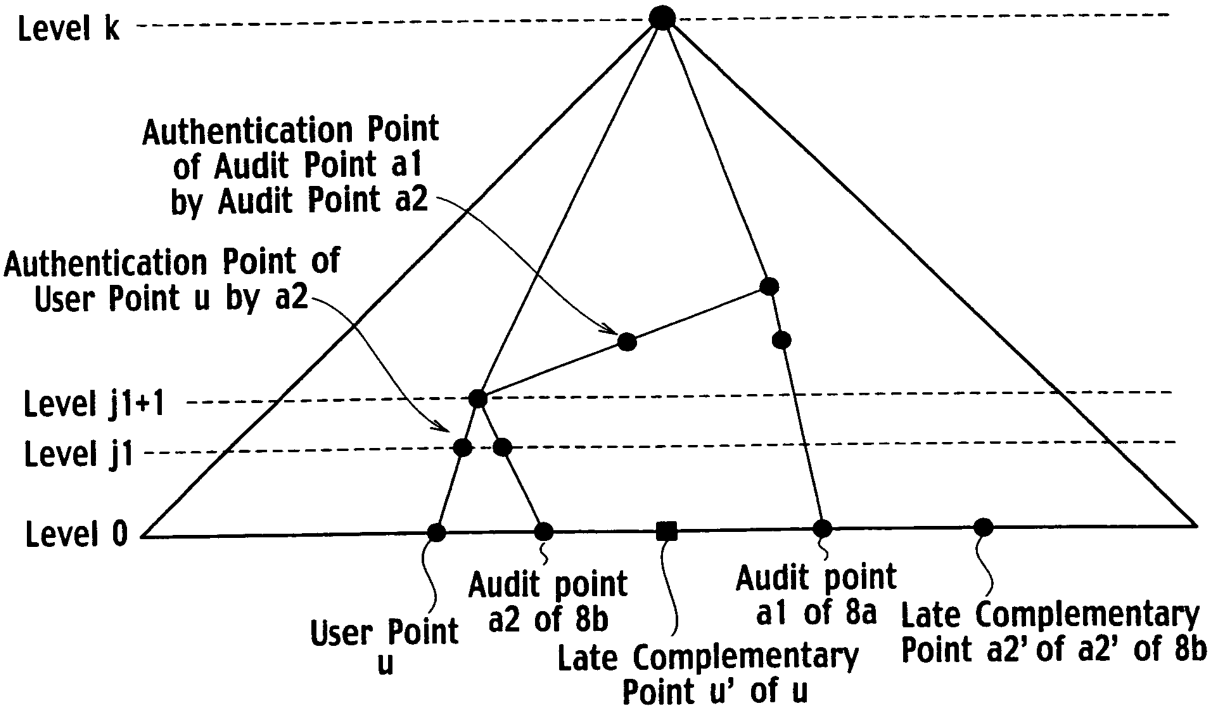

Level k
Authentication Point of Audit Point a1 by Audit Point a2
Authentication Point of User Point u by a2
Level j1+1
Level j1
Level 0
User Point u
Audit point a2 of 8b
Late Complementary Point u' of u
Audit point a1 of 8a
Late Complementary Point a2' of a2' of 8b

FIG. 21

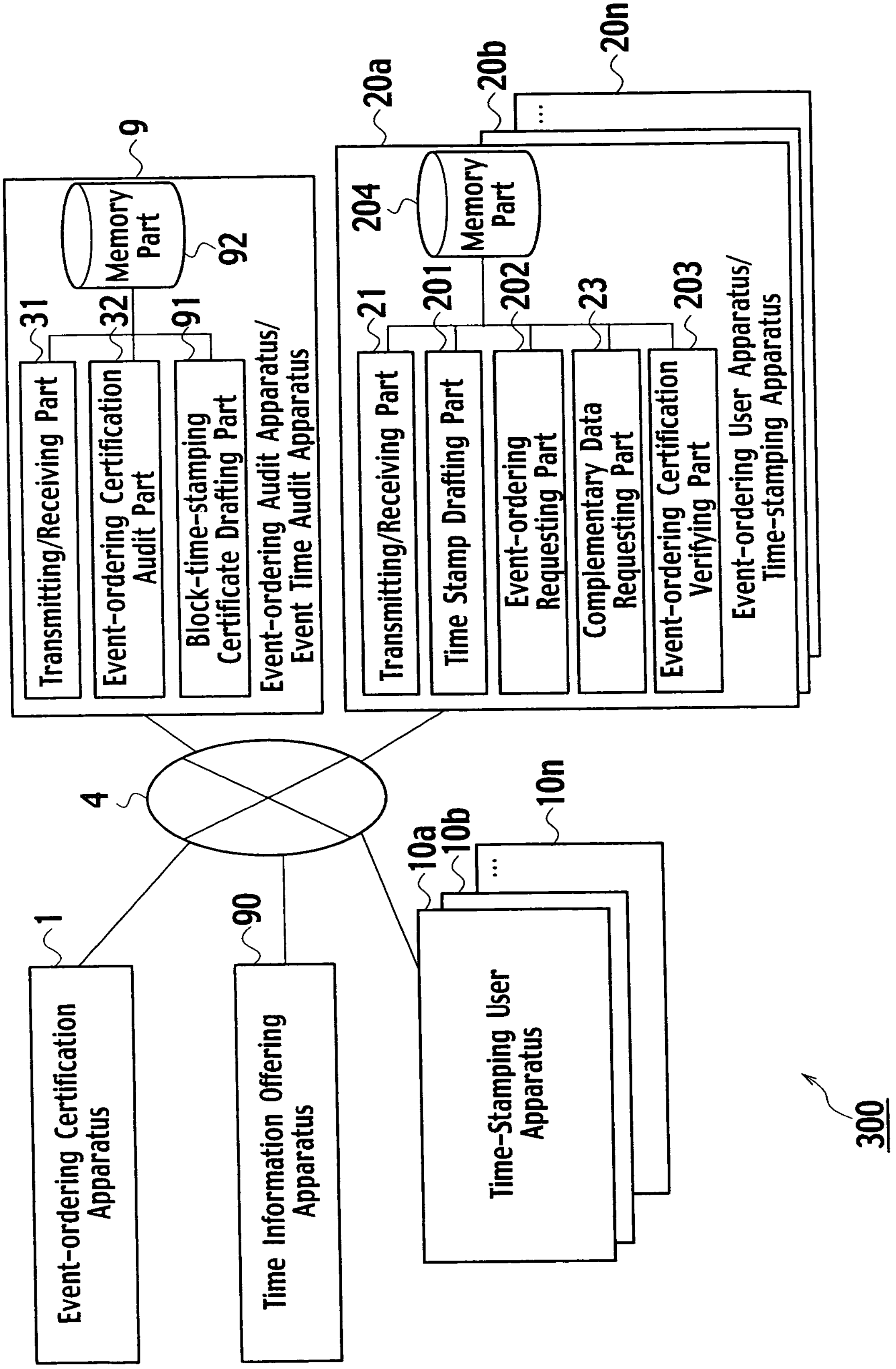

Transmitting/Receiving Part
31
Event-ordering Certification Audit Part
32
Block-time-stamping Certificate Drafting Part
91
Memory Part
92
9
Event-ordering Audit Apparatus/ Event Time Audit Apparatus
Transmitting/Receiving Part
21
Time Stamp Drafting Part
201
Event-ordering Requesting Part
202
Complementary Data Requesting Part
23
Event-ordering Certification Verifying Part
203
Memory Part
204
Event-ordering User Apparatus/ Time-stamping Apparatus
20a
20b
20n
...
4
Event-ordering Certification Apparatus
1
Time Information Offering Apparatus
90
Time-Stamping User Apparatus
10a
10b
10n
...
300

FIG. 22

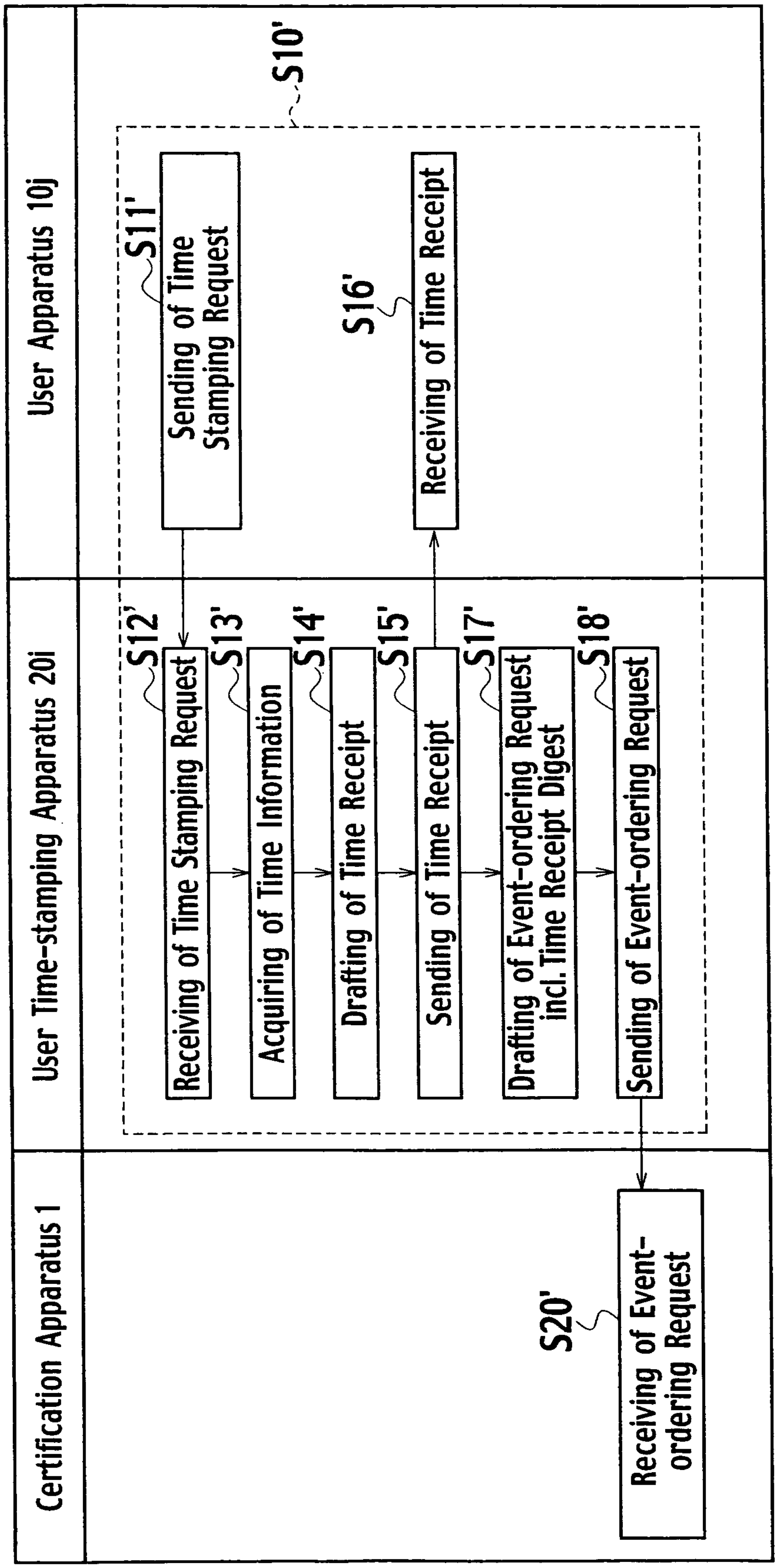

User Apparatus 10j
S10'
S11'
Sending of Time Stamping Request
S16'
Receiving of Time Receipt
User Time-stamping Apparatus 20i
S12'
Receiving of Time Stamping Request
S13'
Acquiring of Time Information
S14'
Drafting of Time Receipt
S15'
Sending of Time Receipt
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S18'
Sending of Event-ordering Request
Certification Apparatus 1
S20'
Receiving of Event-ordering Request

FIG. 23

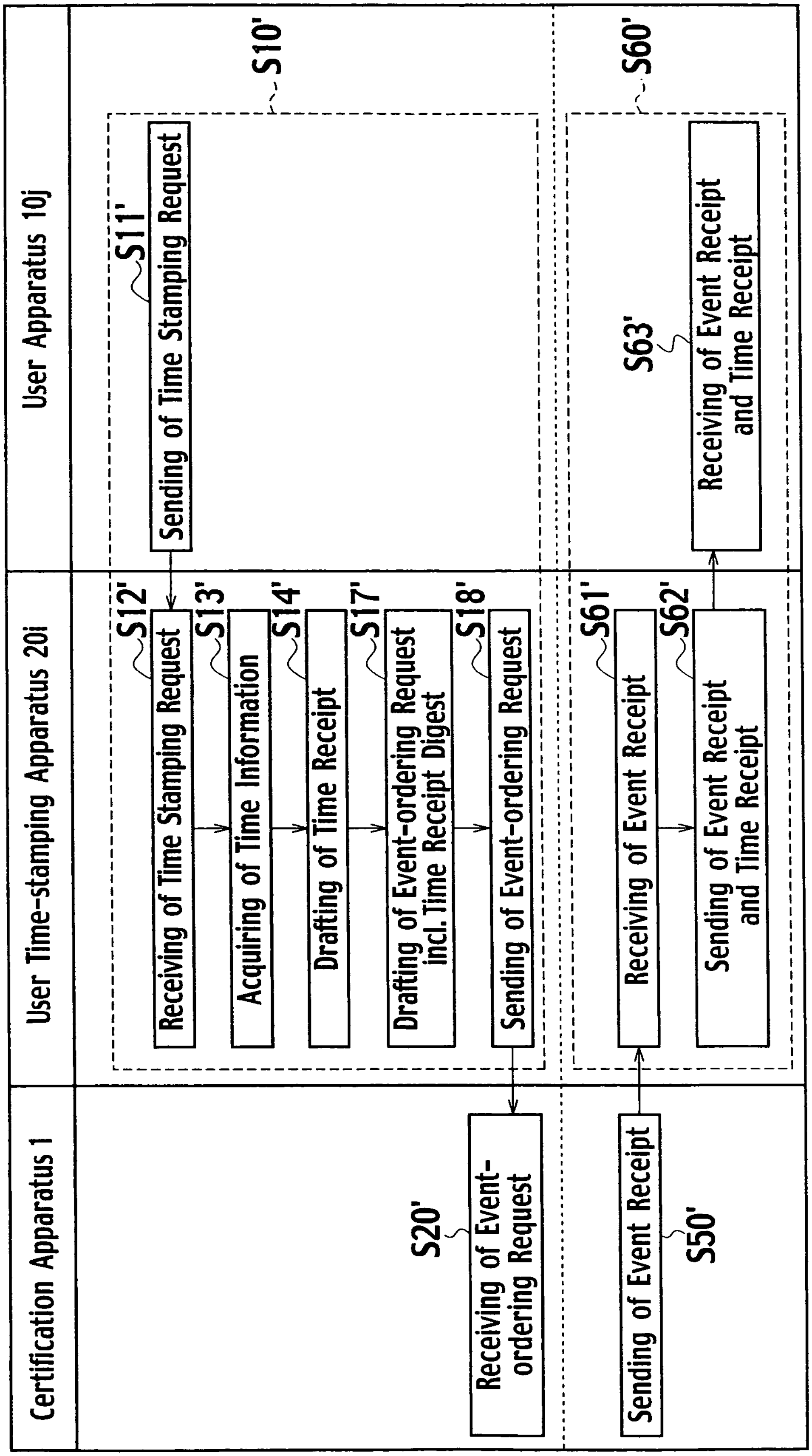

Certification Apparatus 1
User Time-stamping Apparatus 20i
User Apparatus 10j
S10'
S11'
Sending of Time Stamping Request
S12'
Receiving of Time Stamping Request
S13'
Acquiring of Time Information
S14'
Drafting of Time Receipt
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S18'
Sending of Event-ordering Request
S20'
Receiving of Event-ordering Request
S50'
Sending of Event Receipt
S60'
S61'
Receiving of Event Receipt
S62'
Sending of Event Receipt and Time Receipt
S63'
Receiving of Event Receipt and Time Receipt

FIG. 24

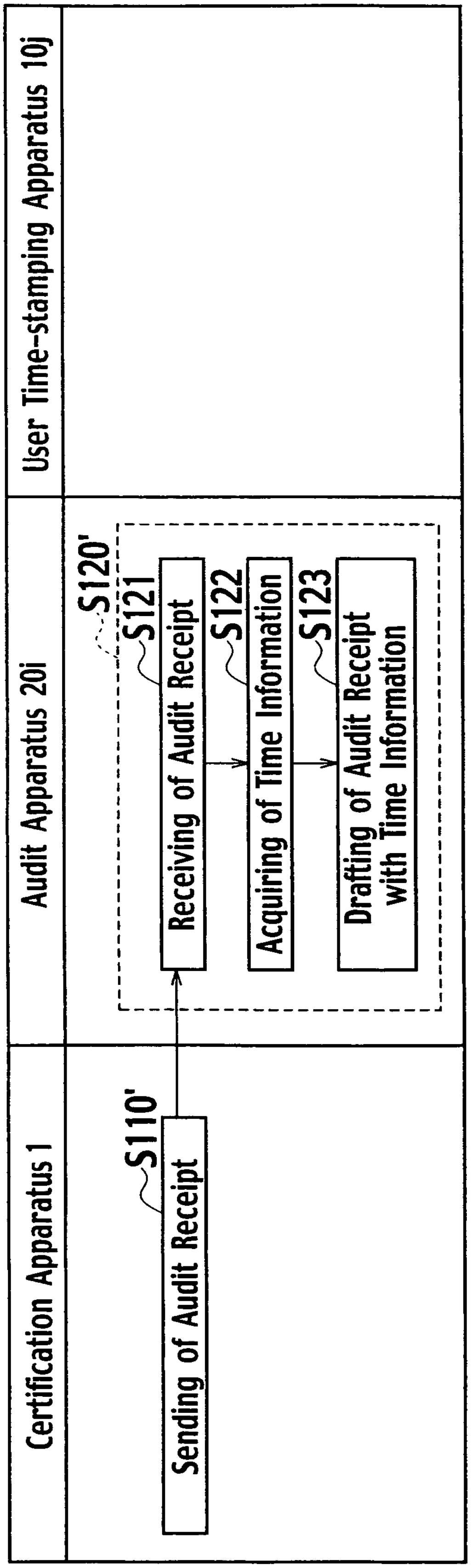

Certification Apparatus 1
Audit Apparatus 20i
User Time-stamping Apparatus 10j
S110'
Sending of Audit Receipt
S120'
S121
Receiving of Audit Receipt
S122
Acquiring of Time Information
S123
Drafting of Audit Receipt with Time Information

FIG. 25

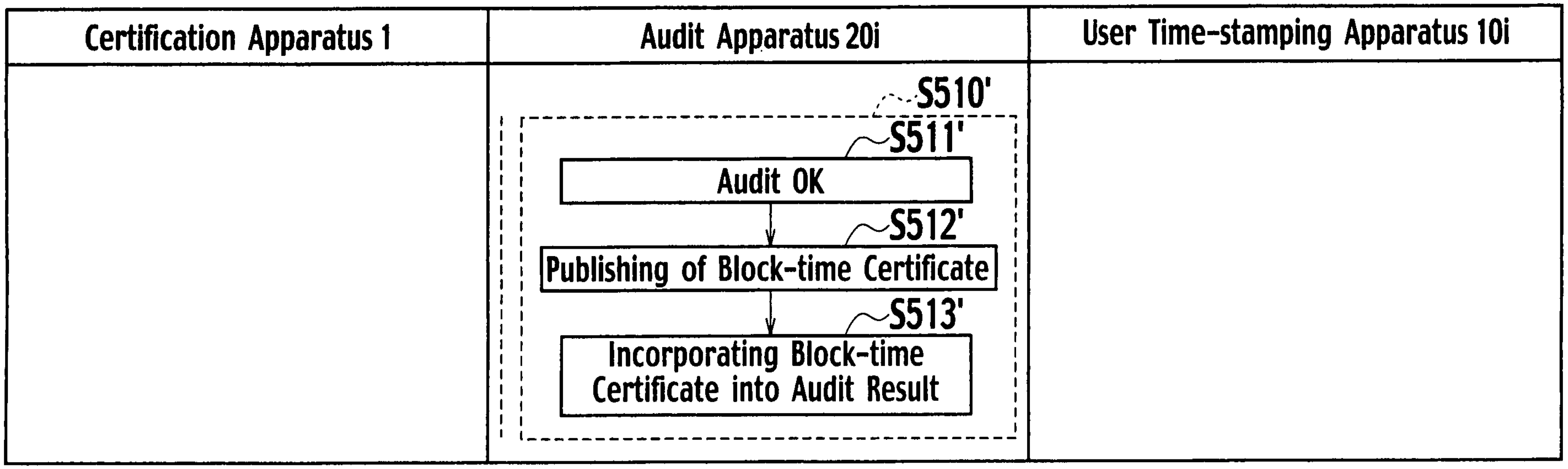

Certification Apparatus 1
Audit Apparatus 20i
User Time-stamping Apparatus 10i
S510'
S511'
Audit OK
S512'
Publishing of Block-time Certificate
S513'
Incorporating Block-time Certificate into Audit Result

FIG. 26

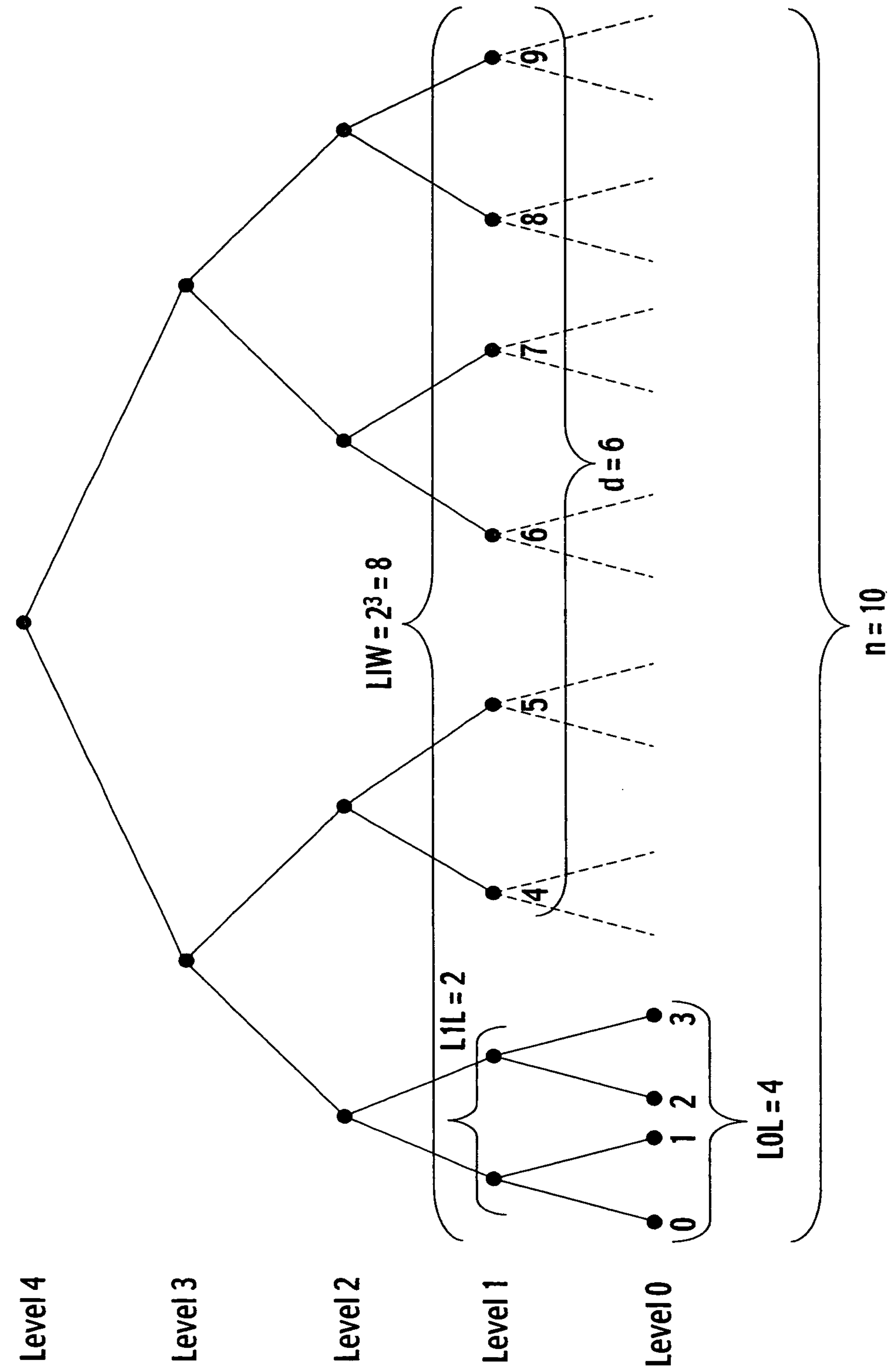

Level 4
Level 3
Level 2
Level 1
Level 0
0
1
2
3
4
5
6
7
8
9
L0L = 4
L1L = 2
LIW = 2^3 = 8
d = 6
n = 10

FIG. 27

```
(1) Loop 1: In a constructive method No. 3, the following processes
            are repeated until a regular time interval is completed.
    (1.1) Setting a request on acceptance to x
    (1.2) Increasing n by increment of 1
    (1.3) Loop 2: Performing of the follow processes for $j=0, ..., k$
        (1.3.1) $i \rightarrow i_j$
        (1.3.2) When $j = 0$, set $A_j[i] := x$.
                (Set x to node($j, i_j$).)
        (1.3.3) When $j > 0$, perform as follows.
            · Set $x0 := A_{j-1}[\mathrm{index}(\mathrm{leftChiild}(j, i))]$
              (Set x0 to an assigned value for left-child of
              node(j, i).)
            · Set $x1 := A_{j-1}[\mathrm{index}(\mathrm{rightChild}(j, i))]$
              (Set x1 to an assigned value for right-child of
              node(j, i).)
            · Calculate $x2 := h(x0 \| x1)$
            · Set $A_j[i] := x2$
              (Assign x2 to node(j, i).)
        (1.3.4) Increasing $i_j$ by increment of 1
        (1.3.5) Withdraw from loop 2 if i is an even number.
     Completion of loop 2
 Completion of loop 1
```

Processing Procedure 1

FIG. 28

```
(2) Performing of the following processes after withdrawing from
    loop 1 on reaching finish time.
  (2.1) Set k:= ceiling($\log_2(n)$).
  (2.2) Calculate rtPath(k, 0, n-1) and Set ((0, r(0), ..., k(, r(k))) to the
        calculation result.
  (2.3) Loop 3:Performing of the follow processes for j=0, ..., k
    (2.3.1) i → $i_j$
    (2.3.2) Case of j = 0:
      (2.3.2.1) When i is an odd number:
        · Produce a dummy r: = R(0, i)
        · Set $A_j[i]$: = r
          (Assign r to node(0, i).)
        · Set $b_j$: = true.
        · Increase $i_j$ by increment of 1.
    (2.3.2) Case of 0<j≦k:
      (2.3.2.1) When i = r(j):
                (when node(j, i) is on rtPath(k, 0, n-1)):
        (2.3.2.1.1) x0:= $A_{j-1}$[index(leftChild (j, i))]
          (Set x0 to an assigned value for left-child of node(j, i).)
        (2.3.2.1.2) x1: = $A_{j-1}$[index(rightChild (j, i))]
          (Set x1 to an assigned value for right-child of node(j, i).)
        (2.3.2.1.3) Calculate x2: = h(x0 || x1)
        (2.3.2.1.4) Set $A_j[i]$: = x2
          (Assign x2 to node(j, i).)
        (2.3.2.1.5) When i is an even number and j < k:
          · Increase i by increment of 1.
          · Calculate r: = R(j, i) and Set $A_j[i]$: = r
            (Assign r to node(j, i).)
          · Set $b_j$: = true.
          · Set $i_j$ : = i + 1
      (2.3.2.2) When i = r(j) + 1, an odd number and j < k:
        · Calculate r: = R(j, i) and Set $A_j[i]$: = r
            (Assign r to node(j, i).)
        · Set $b_j$: = true.
        · Increase $i_j$ by increment of 1.
  Completion of loop 3
```

Processing Procedure 2

FIG. 29

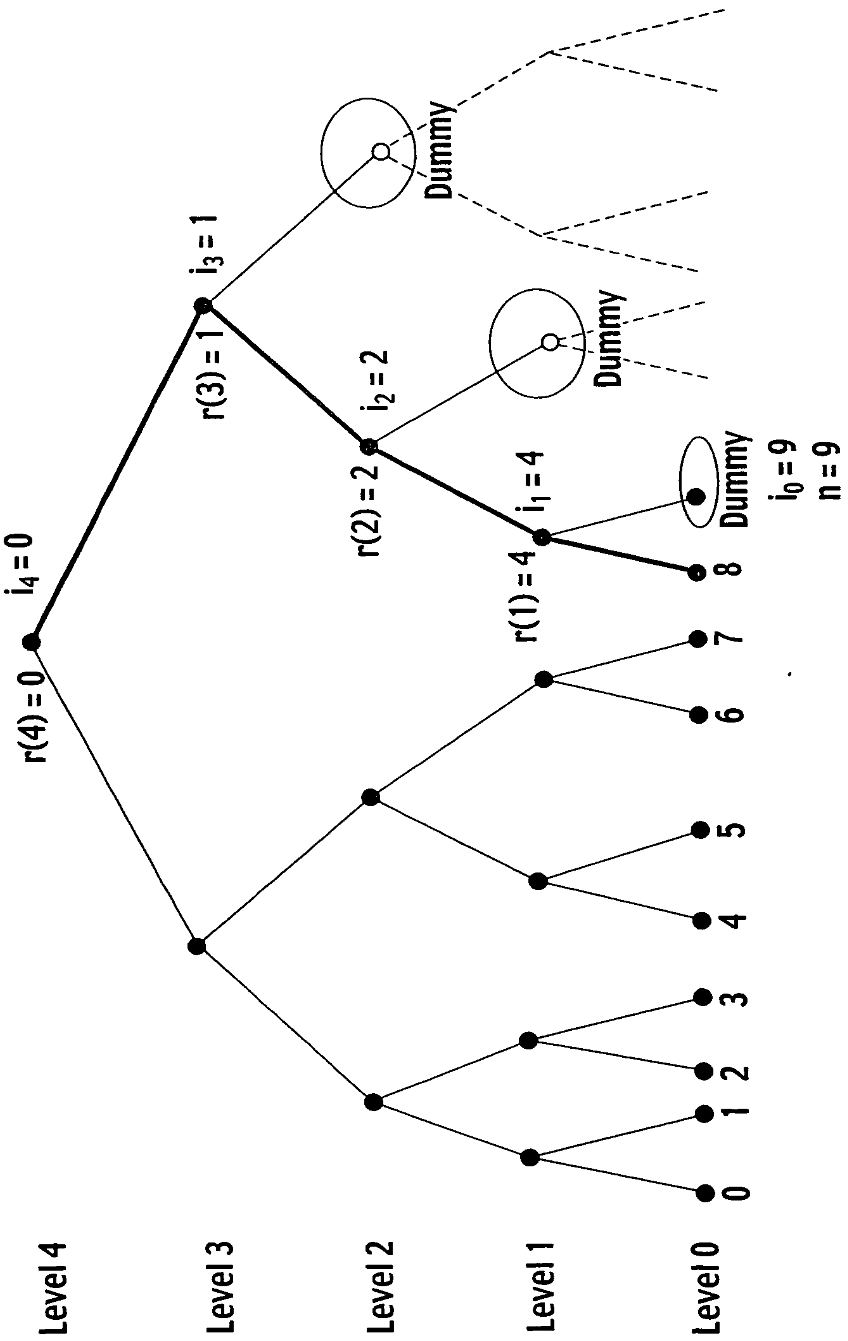

Level 4
Level 3
Level 2
Level 1
Level 0
0
1
2
3
4
5
6
7
8
r(4) = 0
$i_4 = 0$
r(3) = 1
$i_3 = 1$
r(2) = 2
$i_2 = 2$
r(1) = 4
$i_1 = 4$
Dummy
Dummy
Dummy
$i_0 = 9$
n = 9

FIG. 30

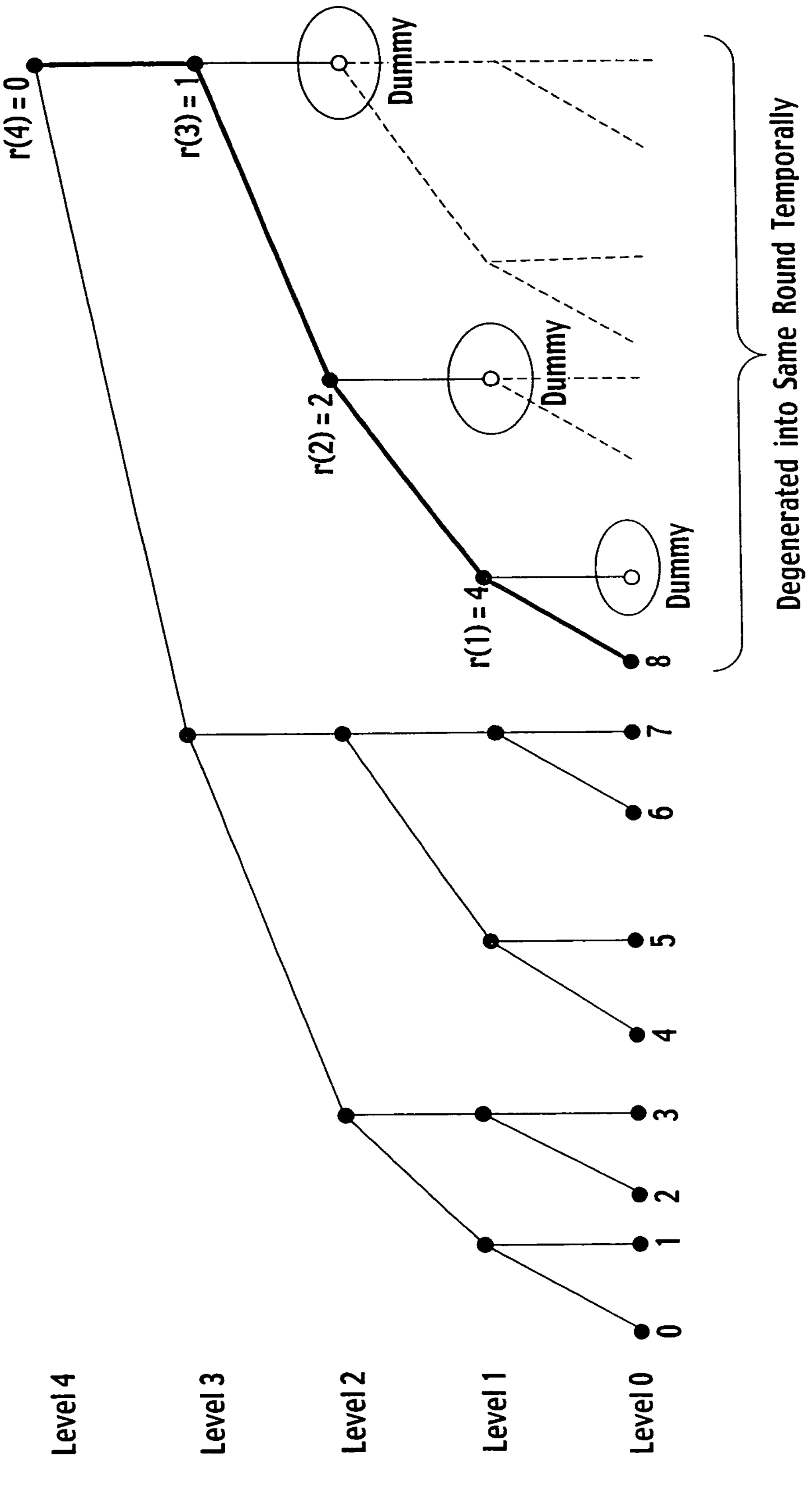

Level 4
Level 3
Level 2
Level 1
Level 0
0
1
2
3
4
5
6
7
8
r(4) = 0
r(3) = 1
r(2) = 2
r(1) = 4
Dummy
Dummy
Dummy
Degenerated into Same Round Temporally

FIG. 31

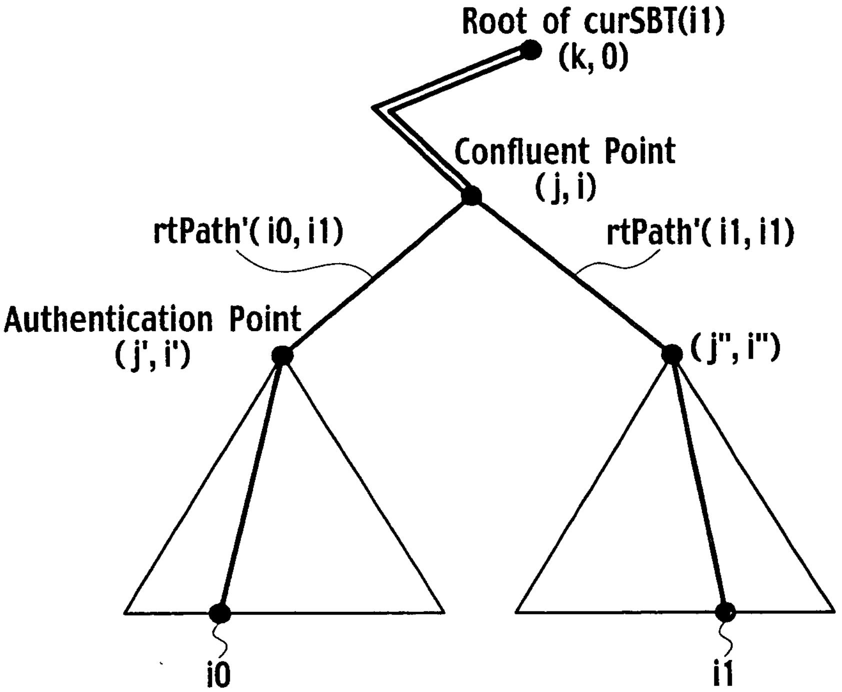

Root of curSBT(i1)
(k, 0)
Confluent Point
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
(j", i")
i0
i1

FIG. 32

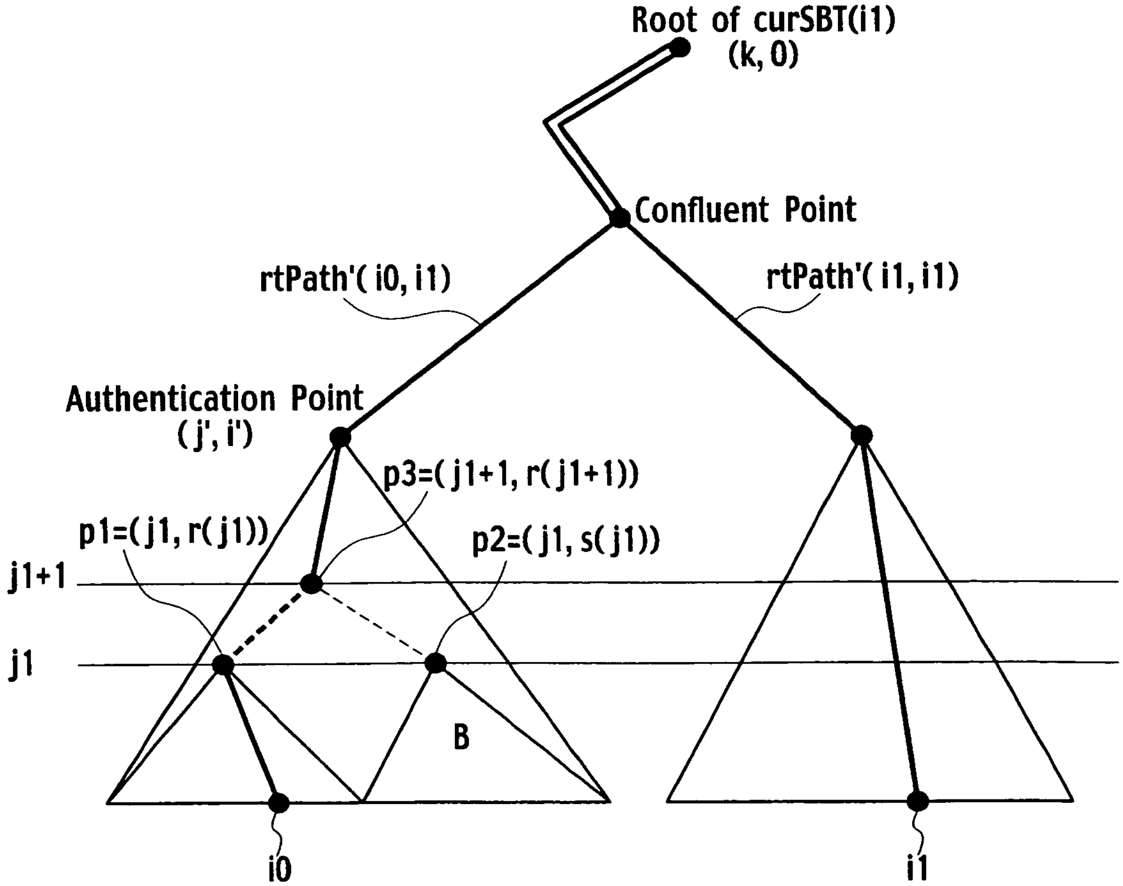

Root of curSBT(i1)
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

FIG. 33

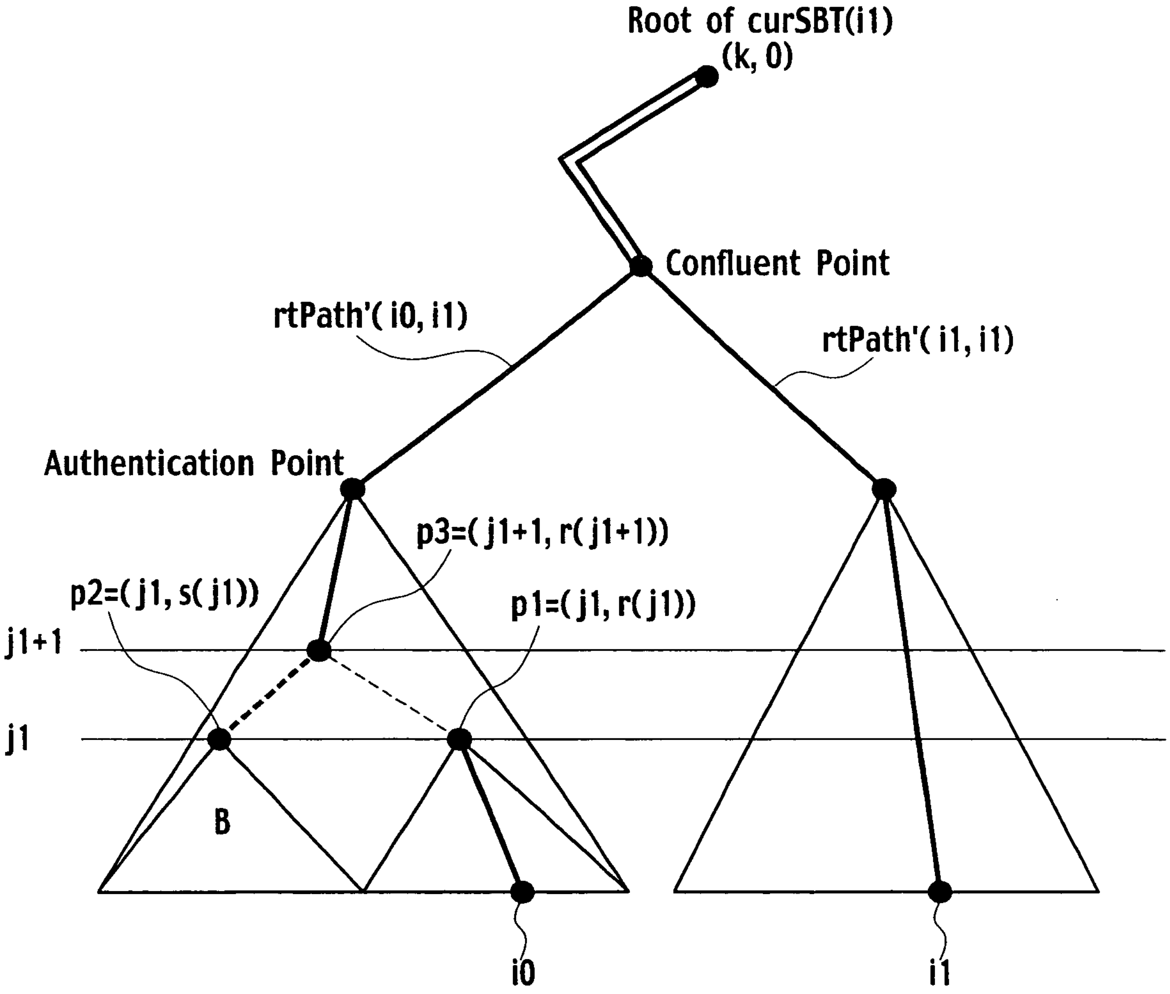

Root of curSBT(i1)
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

FIG. 34

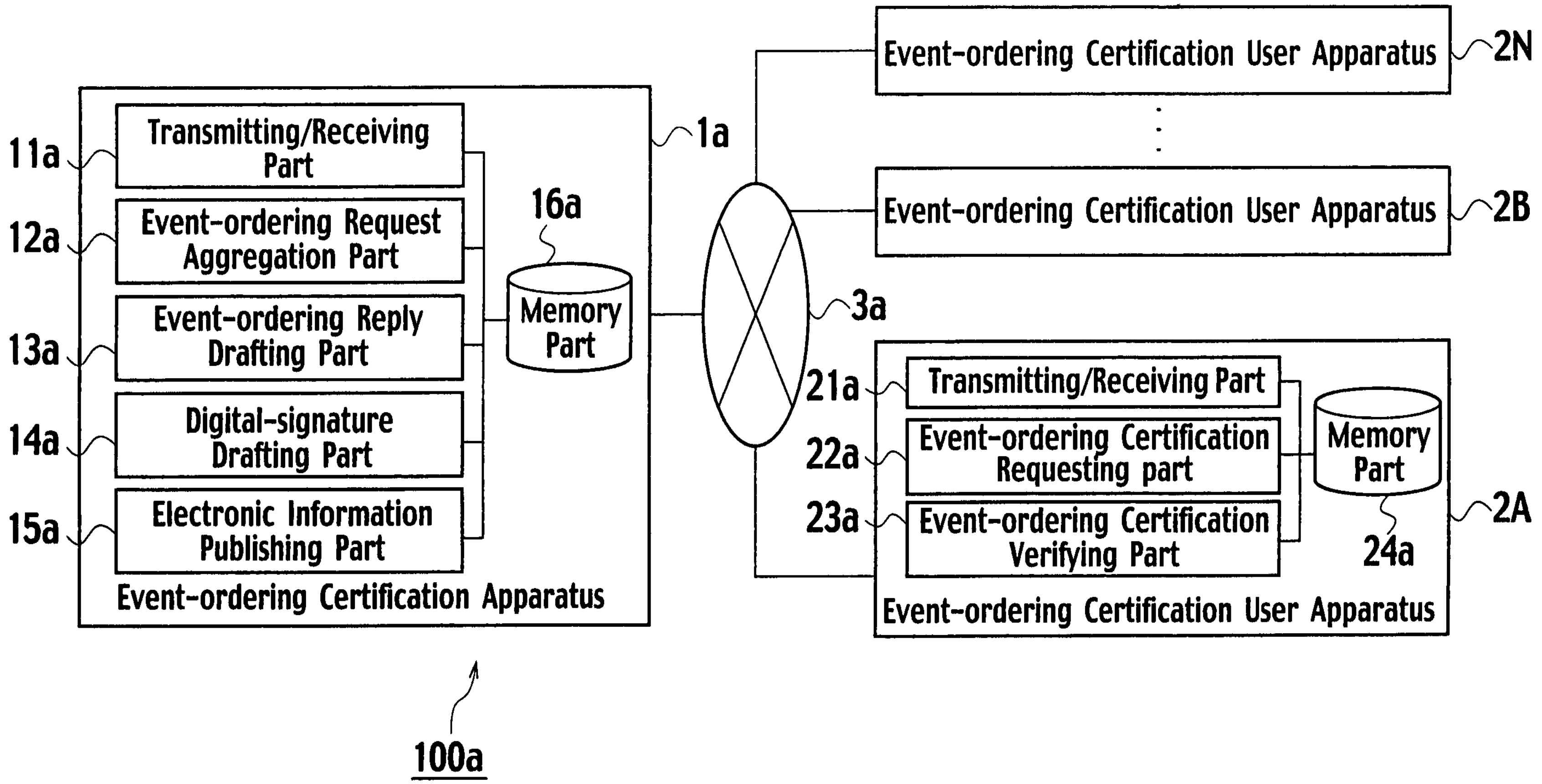

11a
Transmitting/Receiving Part
12a
Event-ordering Request Aggregation Part
13a
Event-ordering Reply Drafting Part
14a
Digital-signature Drafting Part
15a
Electronic Information Publishing Part
16a
Memory Part
Event-ordering Certification Apparatus
1a
100a
3a
Event-ordering Certification User Apparatus
2N
Event-ordering Certification User Apparatus
2B
21a
Transmitting/Receiving Part
22a
Event-ordering Certification Requesting part
23a
Event-ordering Certification Verifying Part
Memory Part
24a
Event-ordering Certification User Apparatus
2A

FIG. 35

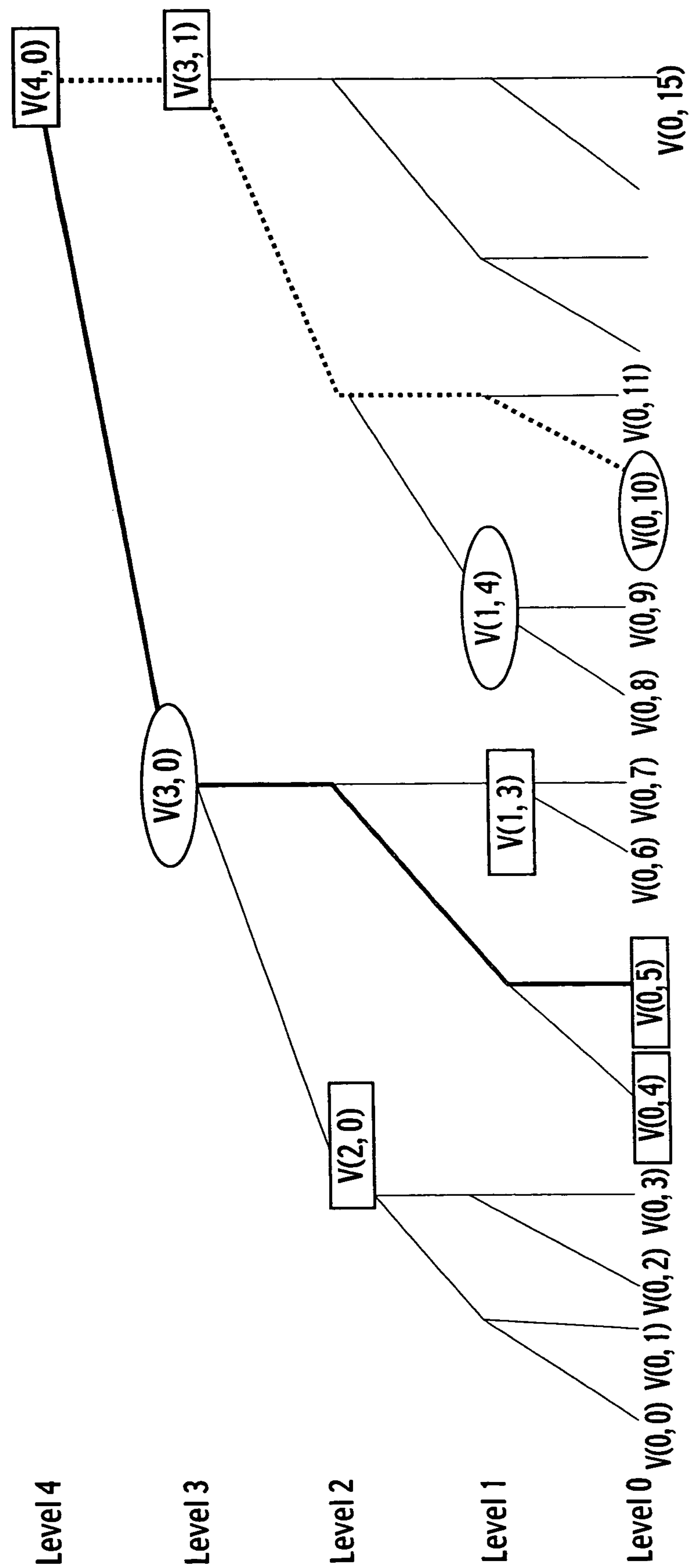

Level 4
Level 3
Level 2
Level 1
Level 0
V(4, 0)
V(3, 1)
V(3, 0)
V(2, 0)
V(1, 3)
V(1, 4)
V(0, 0)
V(0, 1)
V(0, 2)
V(0, 3)
V(0, 4)
V(0, 5)
V(0, 6)
V(0, 7)
V(0, 8)
V(0, 9)
V(0, 10)
V(0, 11)
V(0, 15)

FIG. 36

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○
Late Complementary Data of Each Past Registration Point (Positional Information Assigned Value)	TK	○

Event-ordering Receipt
EOC(y)

FIG. 37

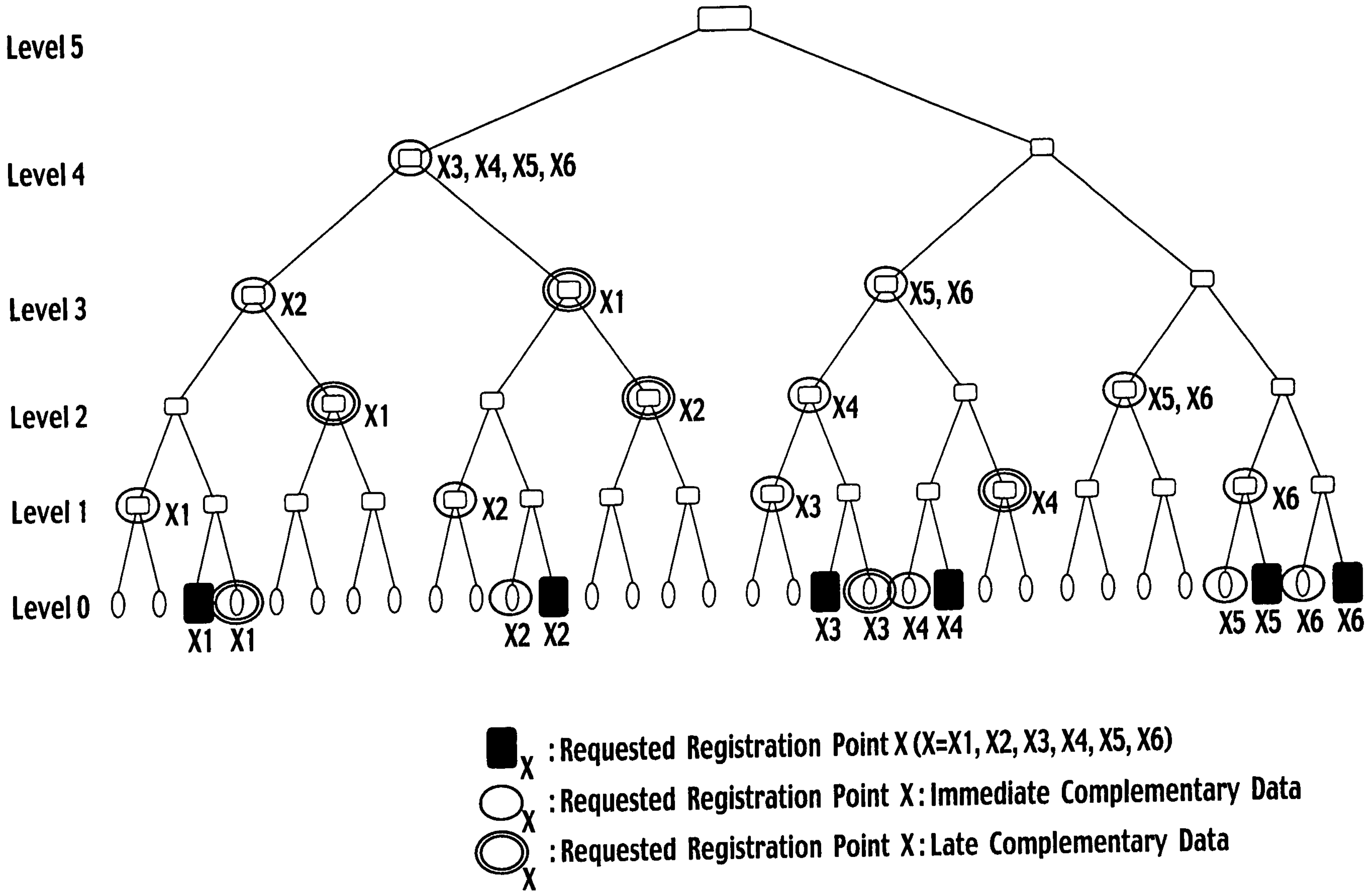

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
X3, X4, X5, X6
X2
X1
X1
X2
X5, X6
X4
X5, X6
X1
X2
X3
X4
X6
X1
X1
X2
X2
X3
X3
X4
X4
X5
X5
X6
X6
■X :Requested Registration Point X (X=X1, X2, X3, X4, X5, X6)
○X :Requested Registration Point X : Immediate Complementary Data
◎X :Requested Registration Point X : Late Complementary Data

FIG. 38

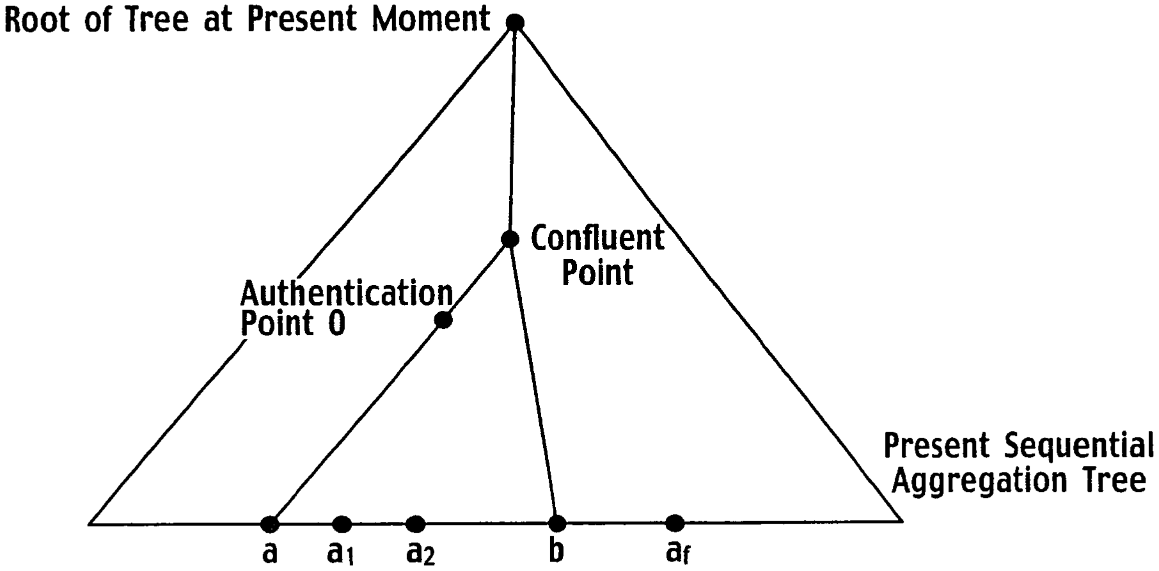

Root of Tree at Present Moment
Confluent Point
Authentication Point 0
Present Sequential Aggregation Tree
a
a1
a2
b
af

FIG. 39

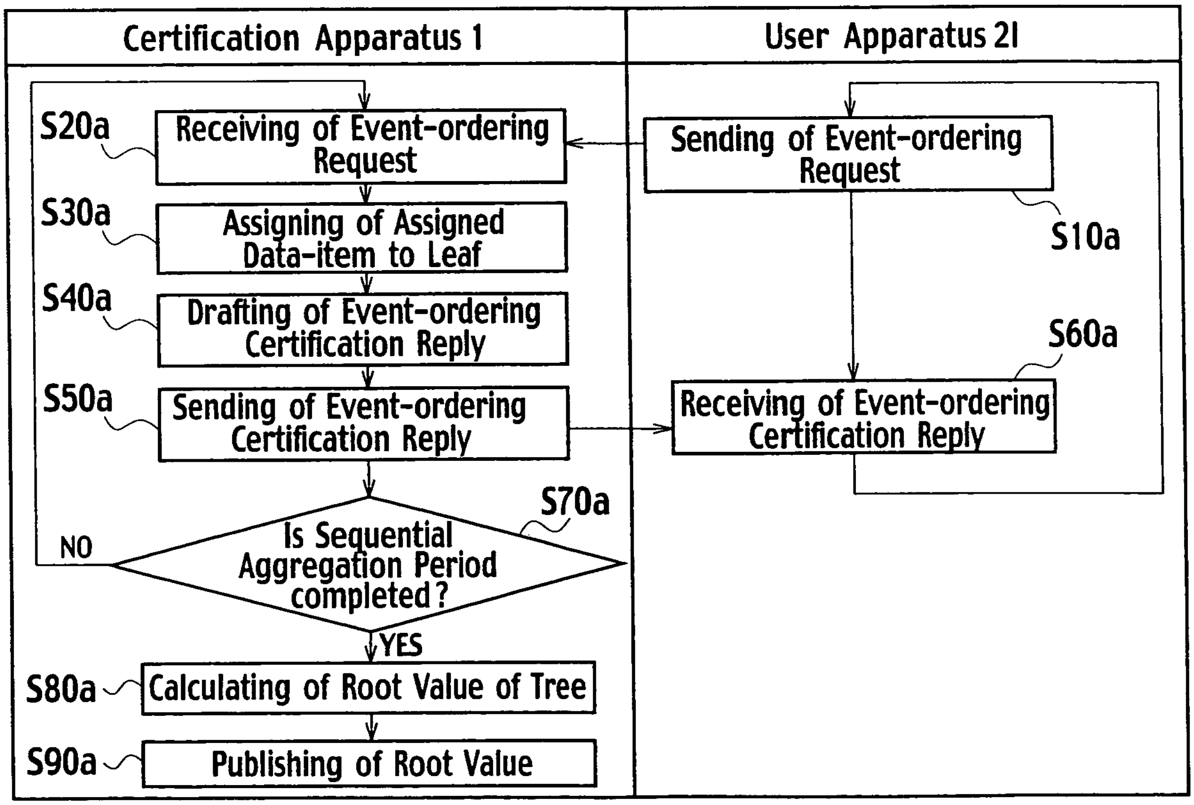

Certification Apparatus 1
User Apparatus 21
S20a
Receiving of Event-ordering Request
S30a
Assigning of Assigned Data-item to Leaf
S40a
Drafting of Event-ordering Certification Reply
S50a
Sending of Event-ordering Certification Reply
S70a
Is Sequential Aggregation Period completed?
NO
YES
S80a
Calculating of Root Value of Tree
S90a
Publishing of Root Value
Sending of Event-ordering Request
S10a
S60a
Receiving of Event-ordering Certification Reply

FIG. 40

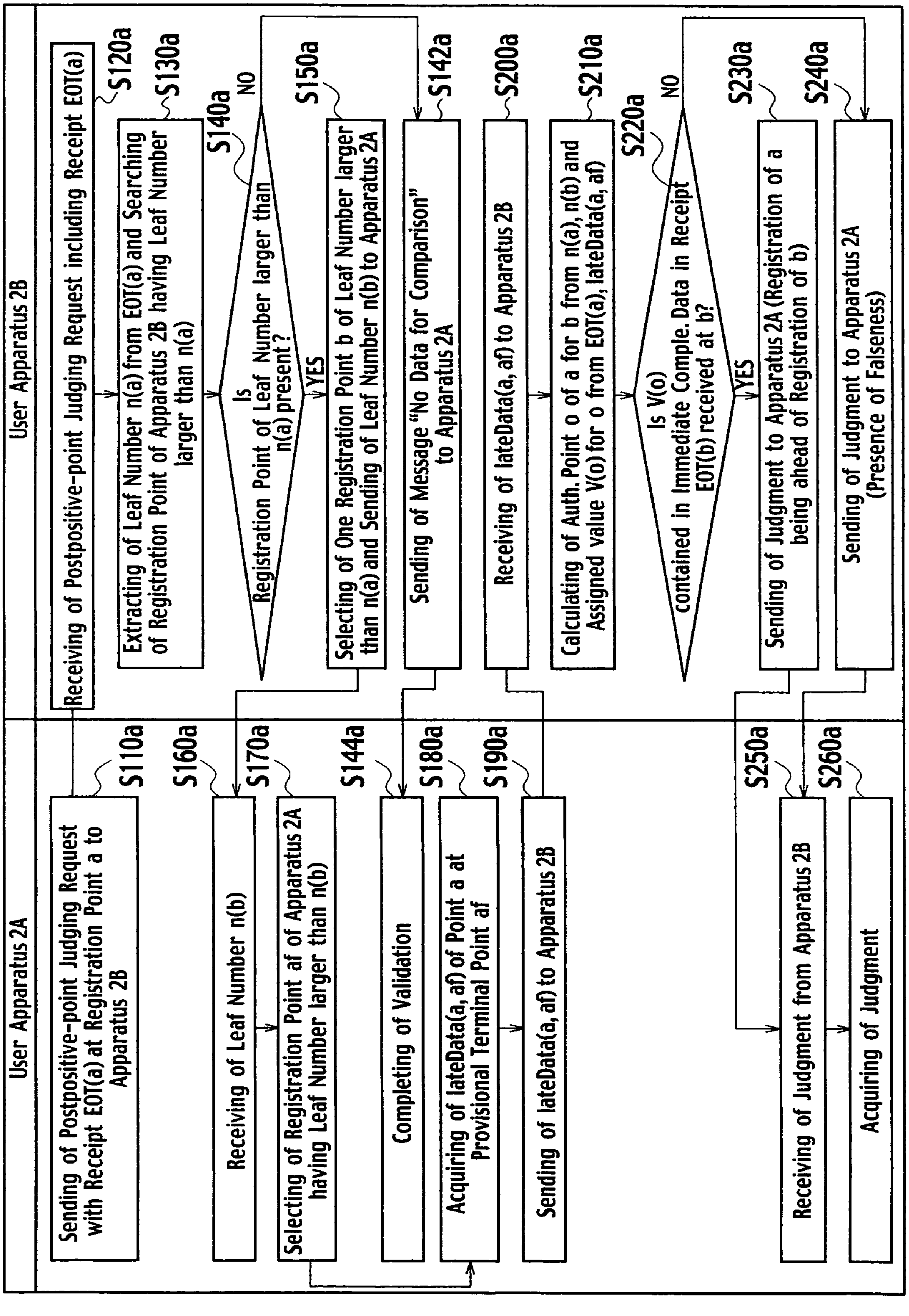

User Apparatus 2A
User Apparatus 2B
Sending of Postpositive-point Judging Request with Receipt EOT(a) at Registration Point a to Apparatus 2B
S110a
Receiving of Postpositive-point Judging Request including Receipt EOT(a)
S120a
Extracting of Leaf Number n(a) from EOT(a) and Searching of Registration Point of Apparatus 2B having Leaf Number larger than n(a)
S130a
Is Registration Point of Leaf Number larger than n(a) present?
S140a
NO
YES
Selecting of One Registration Point b of Leaf Number larger than n(a) and Sending of Leaf Number n(b) to Apparatus 2A
S150a
Sending of Message "No Data for Comparison" to Apparatus 2A
S142a
Receiving of Leaf Number n(b)
S160a
Selecting of Registration Point af of Apparatus 2A having Leaf Number larger than n(b)
S170a
Completing of Validation
S144a
Acquiring of lateData(a, af) of Point a at Provisional Terminal Point af
S180a
Sending of lateData(a, af) to Apparatus 2B
S190a
Receiving of lateData(a, af) to Apparatus 2B
S200a
Calculating of Auth. Point o of a for b from n(a), n(b) and Assigned value V(o) for o from EOT(a), lateData(a, af)
S210a
Is V(o) contained in Immediate Comple. Data in Receipt EOT(b) received at b?
S220a
NO
YES
Sending of Judgment to Apparatus 2A (Registration of a being ahead of Registration of b)
S230a
Sending of Judgment to Apparatus 2A (Presence of Falseness)
S240a
Receiving of Judgment from Apparatus 2B
S250a
Acquiring of Judgment
S260a

FIG. 41

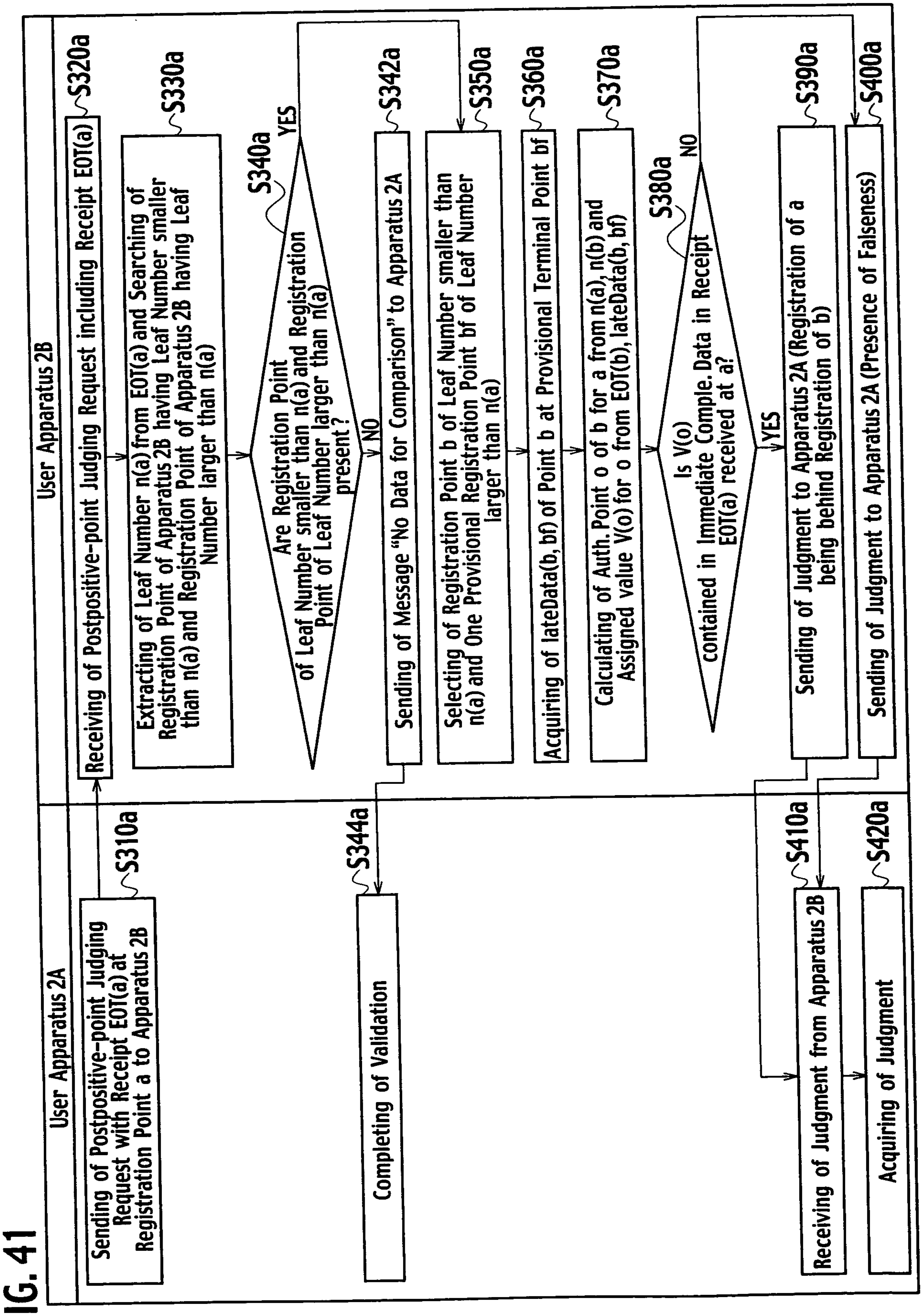

User Apparatus 2A
User Apparatus 2B
Sending of Postpositive-point Judging Request with Receipt EOT(a) at Registration Point a to Apparatus 2B
S310a
Receiving of Postpositive-point Judging Request including Receipt EOT(a)
S320a
Extracting of Leaf Number n(a) from EOT(a) and Searching of Registration Point of Apparatus 2B having Leaf Number smaller than n(a) and Registration Point of Apparatus 2B having Leaf Number larger than n(a)
S330a
Are Registration Point of Leaf Number smaller than n(a) and Registration Point of Leaf Number larger than n(a) present?
S340a
YES
NO
Sending of Message "No Data for Comparison" to Apparatus 2A
S342a
Completing of Validation
S344a
Selecting of Registration Point b of Leaf Number smaller than n(a) and One Provisional Registration Point bf of Leaf Number larger than n(a)
S350a
Acquiring of lateData(b, bf) of Point b at Provisional Terminal Point bf
S360a
Calculating of Auth. Point o of b for a from n(a), n(b) and Assigned value V(o) for o from EOT(b), lateData(b, bf)
S370a
Is V(o) contained in Immediate Comple. Data in Receipt EOT(a) received at a?
S380a
NO
YES
Sending of Judgment to Apparatus 2A (Registration of a being behind Registration of b)
S390a
Sending of Judgment to Apparatus 2A (Presence of Falseness)
S400a
Receiving of Judgment from Apparatus 2B
S410a
Acquiring of Judgment
S420a

FIG. 42

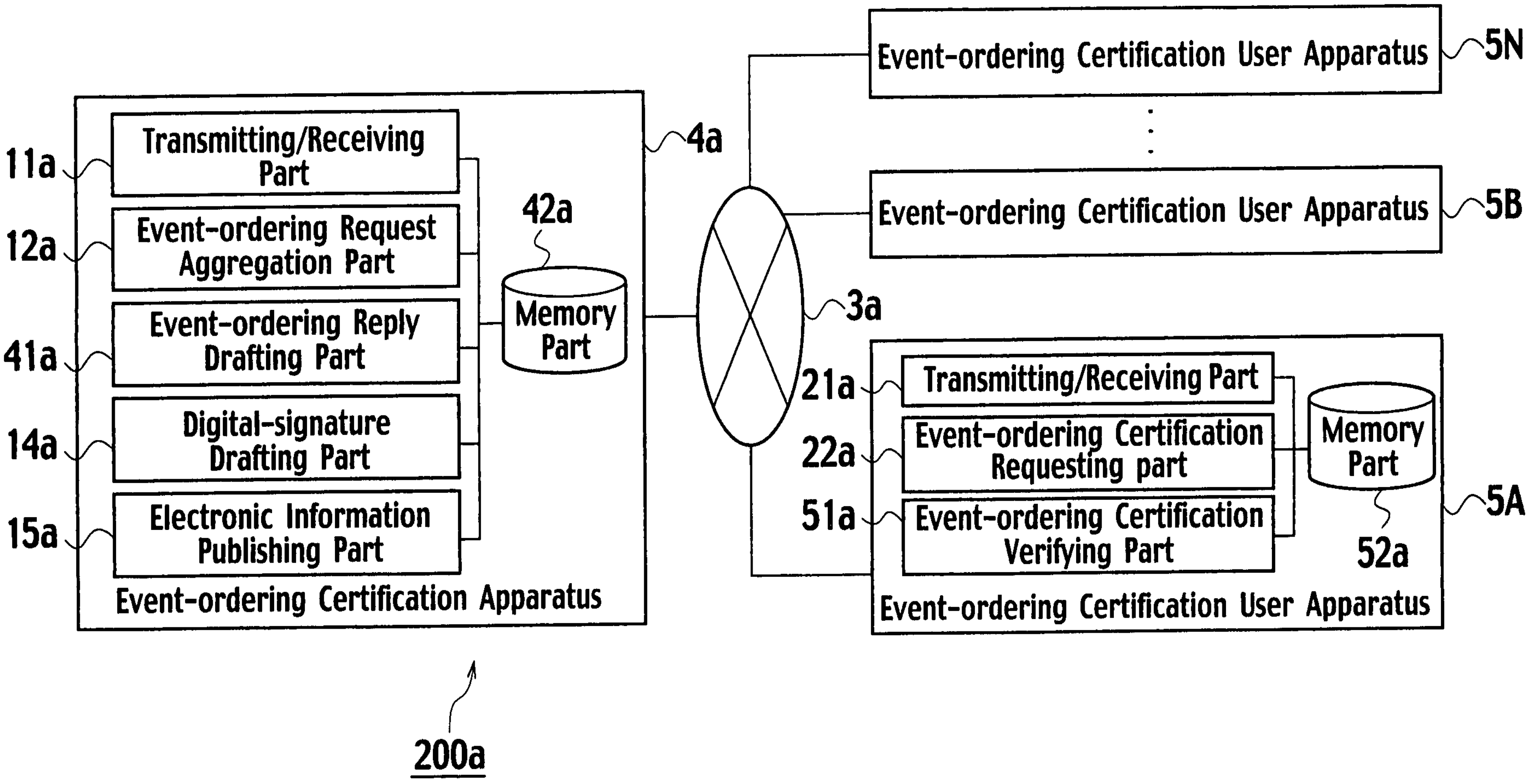

11a
Transmitting/Receiving Part
12a
Event-ordering Request Aggregation Part
41a
Event-ordering Reply Drafting Part
14a
Digital-signature Drafting Part
15a
Electronic Information Publishing Part
42a
Memory Part
Event-ordering Certification Apparatus
4a
200a
3a
Event-ordering Certification User Apparatus
5N
Event-ordering Certification User Apparatus
5B
21a
Transmitting/Receiving Part
22a
Event-ordering Certification Requesting part
51a
Event-ordering Certification Verifying Part
Memory Part
52a
Event-ordering Certification User Apparatus
5A

FIG. 43

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○
Late Complementary Data of Immediately-preceding Registration Point (Positional Information Assigned Value)	TK2	○

Event-ordering Receipt EOC(y)

FIG. 44

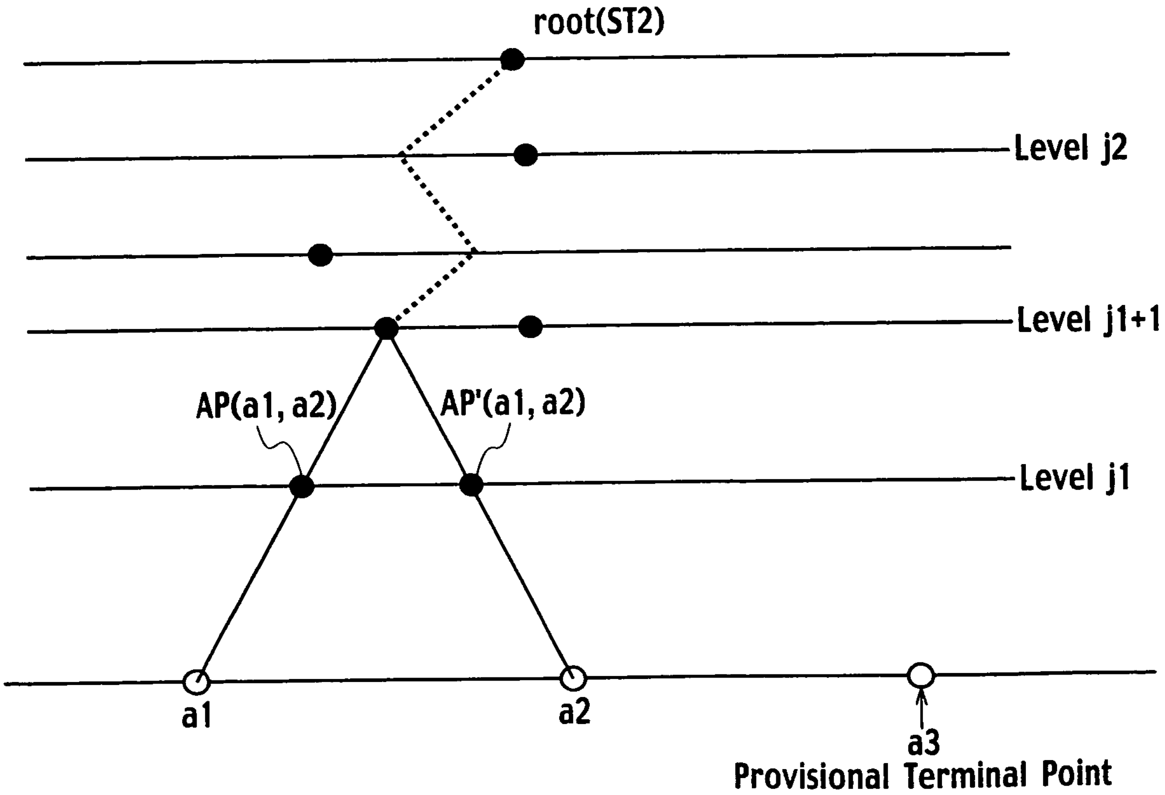


FIG. 45

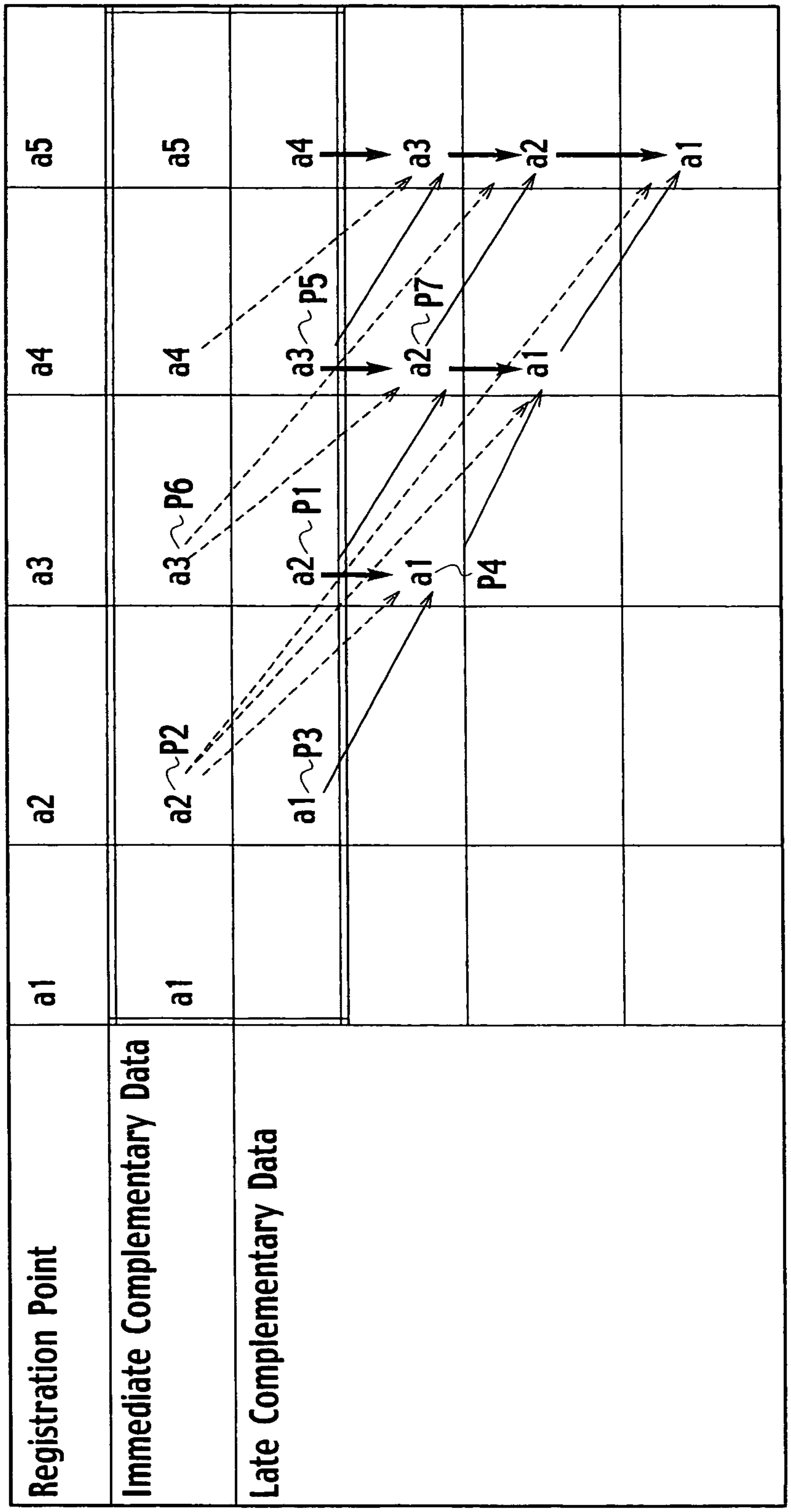
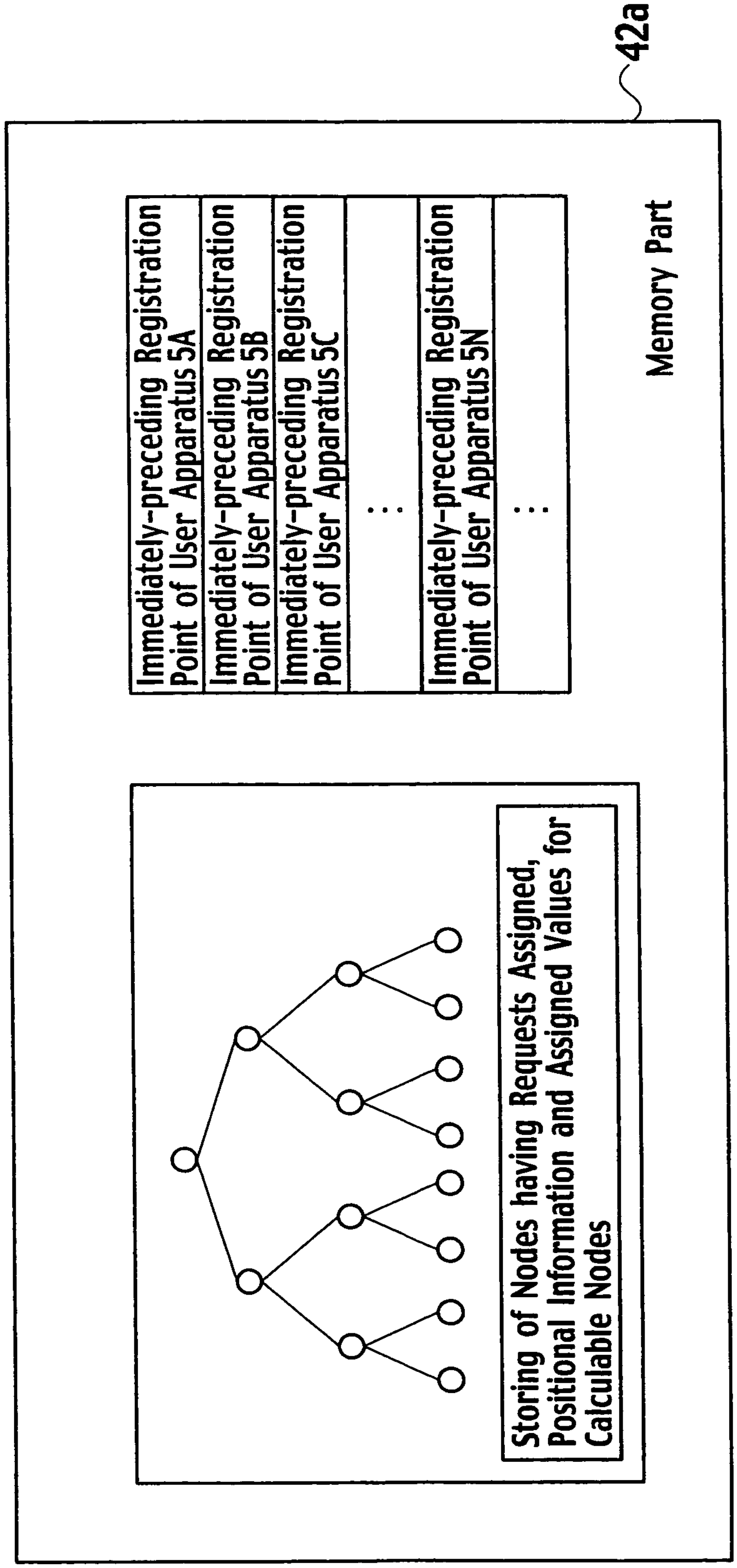

Registration Point
a1
a2
a3
a4
a5
Immediate Complementary Data
a1
a2
P2
a3
P6
a4
a5
Late Complementary Data
a1
P3
a2
P1
a3
P5
a4
a1
P4
a2
P7
a3
a1
a2
a1

FIG. 46


42a
Memory Part
Storing of Nodes having Requests Assigned, Positional Information and Assigned Values for Calculable Nodes

Immediately-preceding Registration Point of User Apparatus 5A

Immediately-preceding Registration Point of User Apparatus 5B

Immediately-preceding Registration Point of User Apparatus 5C

...

Immediately-preceding Registration Point of User Apparatus 5N

...

FIG. 47

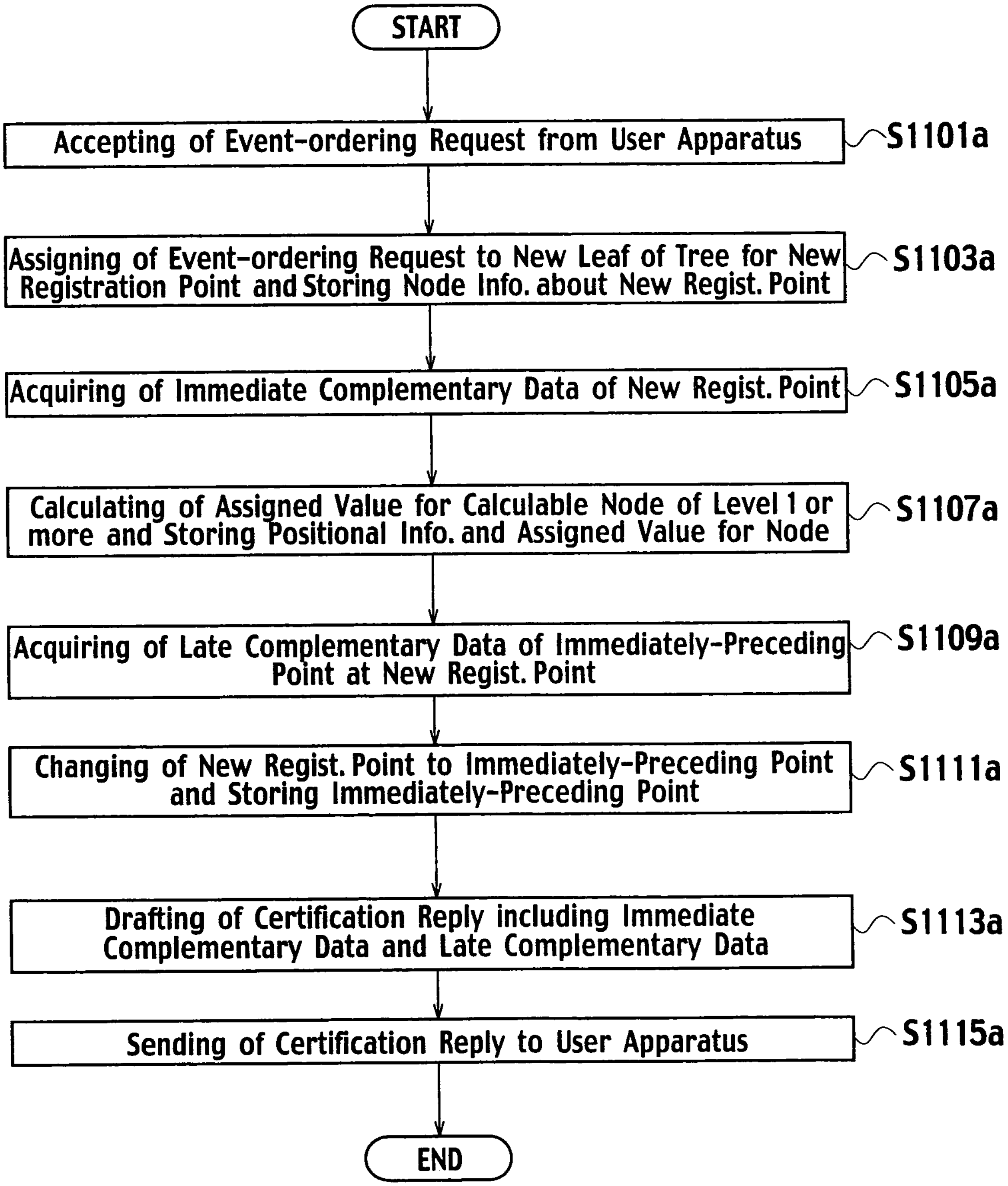

START
Accepting of Event-ordering Request from User Apparatus
S1101a
Assigning of Event-ordering Request to New Leaf of Tree for New Registration Point and Storing Node Info. about New Regist. Point
S1103a
Acquiring of Immediate Complementary Data of New Regist. Point
S1105a
Calculating of Assigned Value for Calculable Node of Level 1 or more and Storing Positional Info. and Assigned Value for Node
S1107a
Acquiring of Late Complementary Data of Immediately-Preceding Point at New Regist. Point
S1109a
Changing of New Regist. Point to Immediately-Preceding Point and Storing Immediately-Preceding Point
S1111a
Drafting of Certification Reply including Immediate Complementary Data and Late Complementary Data
S1113a
Sending of Certification Reply to User Apparatus
S1115a
END

FIG. 48

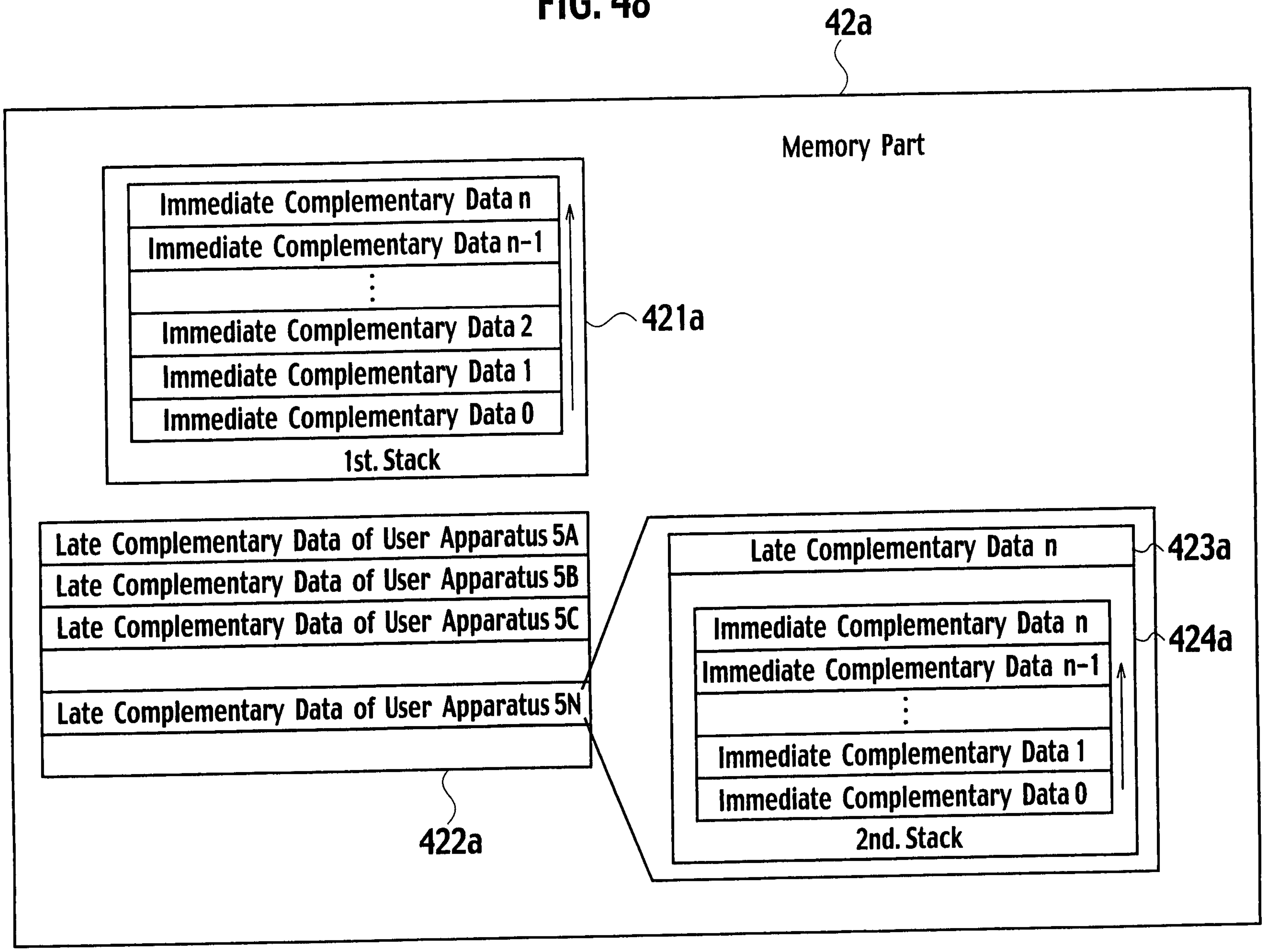

42a
Memory Part
Immediate Complementary Data n
Immediate Complementary Data n-1
⋮
Immediate Complementary Data 2
Immediate Complementary Data 1
Immediate Complementary Data 0
1st. Stack
421a
Late Complementary Data of User Apparatus 5A
Late Complementary Data of User Apparatus 5B
Late Complementary Data of User Apparatus 5C
Late Complementary Data of User Apparatus 5N
422a
Late Complementary Data n
423a
Immediate Complementary Data n
Immediate Complementary Data n-1
⋮
Immediate Complementary Data 1
Immediate Complementary Data 0
424a
2nd. Stack

FIG. 49

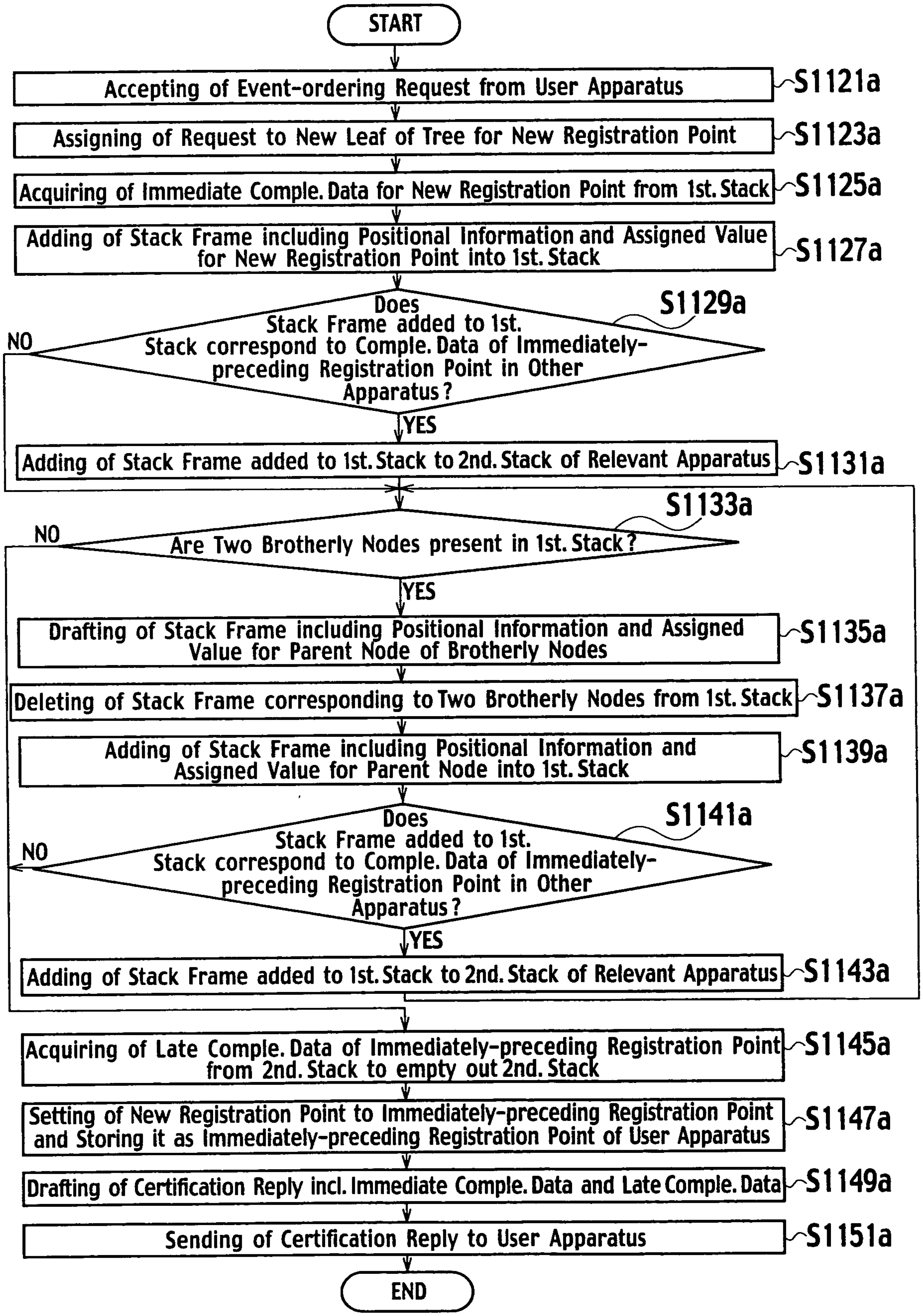

START
Accepting of Event-ordering Request from User Apparatus
S1121a
Assigning of Request to New Leaf of Tree for New Registration Point
S1123a
Acquiring of Immediate Comple. Data for New Registration Point from 1st. Stack
S1125a
Adding of Stack Frame including Positional Information and Assigned Value for New Registration Point into 1st. Stack
S1127a
Does Stack Frame added to 1st. Stack correspond to Comple. Data of Immediately-preceding Registration Point in Other Apparatus?
S1129a
NO
YES
Adding of Stack Frame added to 1st. Stack to 2nd. Stack of Relevant Apparatus
S1131a
Are Two Brotherly Nodes present in 1st. Stack?
S1133a
NO
YES
Drafting of Stack Frame including Positional Information and Assigned Value for Parent Node of Brotherly Nodes
S1135a
Deleting of Stack Frame corresponding to Two Brotherly Nodes from 1st. Stack
S1137a
Adding of Stack Frame including Positional Information and Assigned Value for Parent Node into 1st. Stack
S1139a
Does Stack Frame added to 1st. Stack correspond to Comple. Data of Immediately-preceding Registration Point in Other Apparatus?
S1141a
NO
YES
Adding of Stack Frame added to 1st. Stack to 2nd. Stack of Relevant Apparatus
S1143a
Acquiring of Late Comple. Data of Immediately-preceding Registration Point from 2nd. Stack to empty out 2nd. Stack
S1145a
Setting of New Registration Point to Immediately-preceding Registration Point and Storing it as Immediately-preceding Registration Point of User Apparatus
S1147a
Drafting of Certification Reply incl. Immediate Comple. Data and Late Comple. Data
S1149a
Sending of Certification Reply to User Apparatus
S1151a
END

FIG. 50

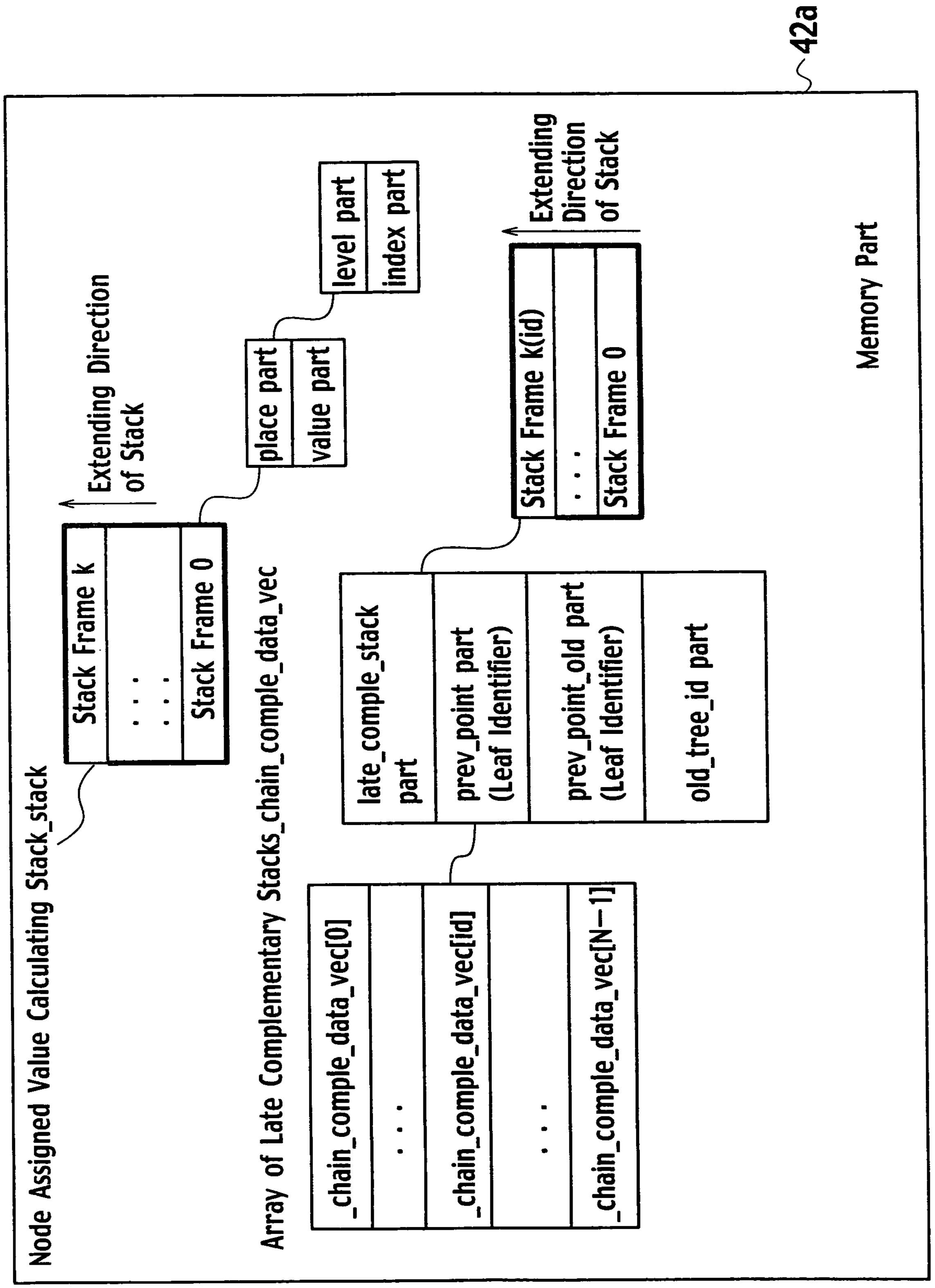

42a
Node Assigned Value Calculating Stack_stack
Stack Frame k
. . .
Stack Frame 0
Extending Direction of Stack
place part
value part
level part
index part
Array of Late Complementary Stacks_chain_comple_data_vec
late_comple_stack part
prev_point_part (Leaf Identifier)
prev_point_old part (Leaf Identifier)
old_tree_id part
Stack Frame k(id)
. . .
Stack Frame 0
Extending Direction of Stack
_chain_comple_data_vec[0]
. . .
_chain_comple_data_vec[id]
. . .
_chain_comple_data_vec[N−1]
Memory Part

FIG. 51

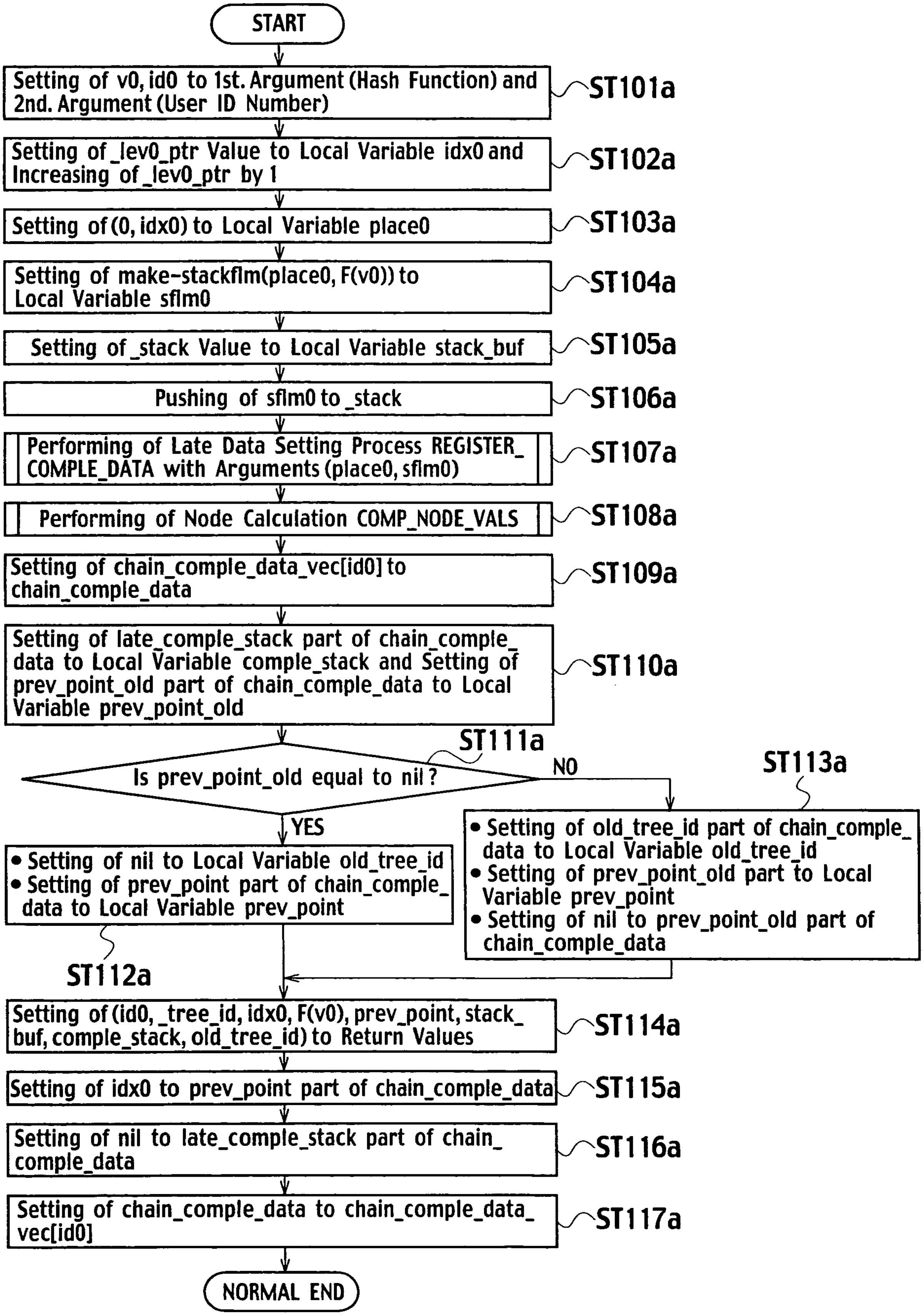

START
Setting of v0, id0 to 1st. Argument (Hash Function) and 2nd. Argument (User ID Number)
ST101a
Setting of _lev0_ptr Value to Local Variable idx0 and Increasing of _lev0_ptr by 1
ST102a
Setting of (0, idx0) to Local Variable place0
ST103a
Setting of make-stackflm(place0, F(v0)) to Local Variable sflm0
ST104a
Setting of _stack Value to Local Variable stack_buf
ST105a
Pushing of sflm0 to _stack
ST106a
Performing of Late Data Setting Process REGISTER_COMPLE_DATA with Arguments (place0, sflm0)
ST107a
Performing of Node Calculation COMP_NODE_VALS
ST108a
Setting of chain_comple_data_vec[id0] to chain_comple_data
ST109a
Setting of late_comple_stack part of chain_comple_data to Local Variable comple_stack and Setting of prev_point_old part of chain_comple_data to Local Variable prev_point_old
ST110a
ST111a
Is prev_point_old equal to nil?
NO
ST113a
YES
• Setting of nil to Local Variable old_tree_id
• Setting of prev_point part of chain_comple_data to Local Variable prev_point
• Setting of old_tree_id part of chain_comple_data to Local Variable old_tree_id
• Setting of prev_point_old part to Local Variable prev_point
• Setting of nil to prev_point_old part of chain_comple_data
ST112a
Setting of (id0, _tree_id, idx0, F(v0), prev_point, stack_buf, comple_stack, old_tree_id) to Return Values
ST114a
Setting of idx0 to prev_point part of chain_comple_data
ST115a
Setting of nil to late_comple_stack part of chain_comple_data
ST116a
Setting of chain_comple_data to chain_comple_data_vec[id0]
ST117a
NORMAL END

FIG. 52

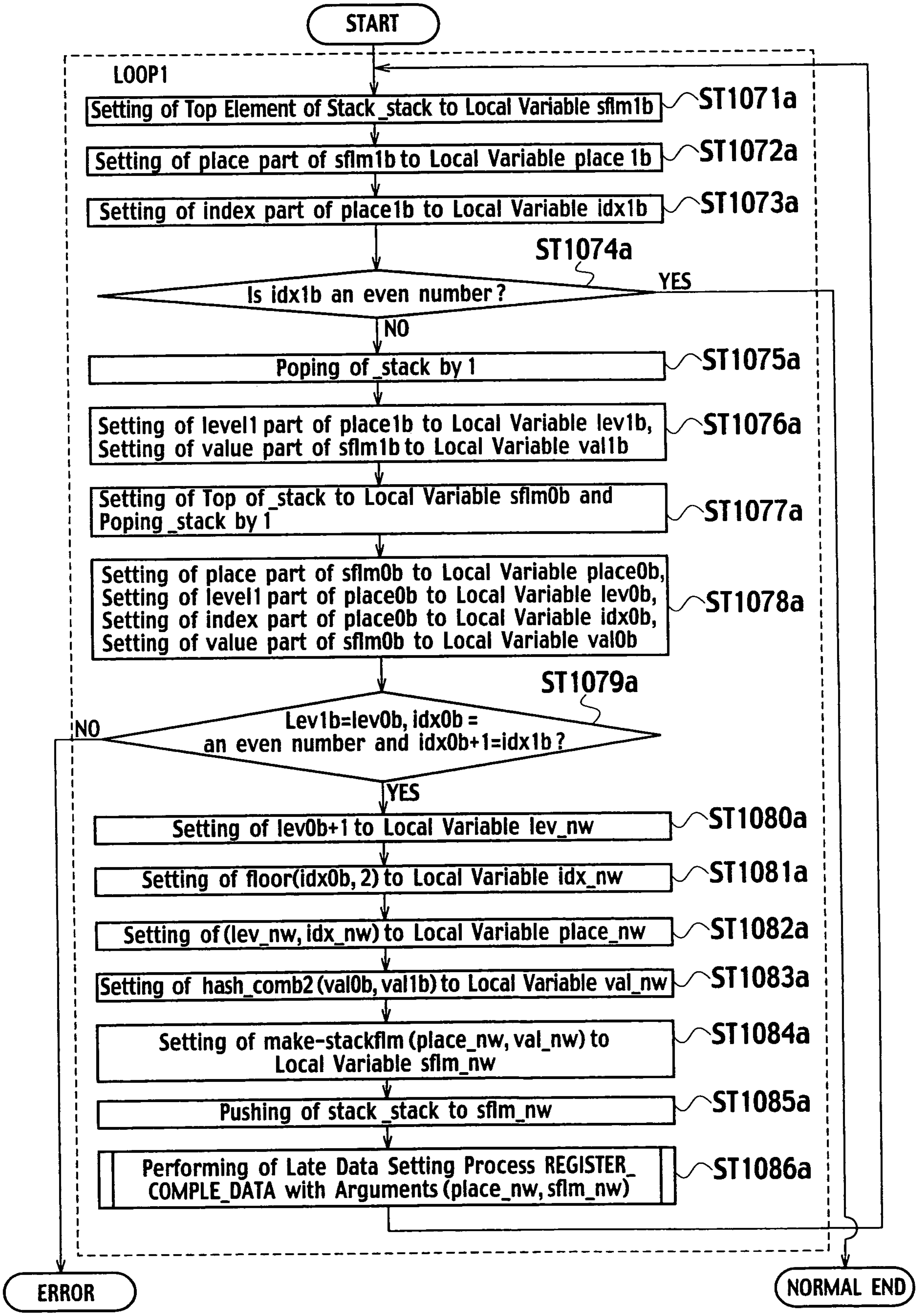

START
LOOP1
Setting of Top Element of Stack _stack to Local Variable sflm1b
ST1071a
Setting of place part of sflm1b to Local Variable place1b
ST1072a
Setting of index part of place1b to Local Variable idx1b
ST1073a
ST1074a
Is idx1b an even number?
YES
NO
Poping of _stack by 1
ST1075a
Setting of level1 part of place1b to Local Variable lev1b,
Setting of value part of sflm1b to Local Variable val1b
ST1076a
Setting of Top of _stack to Local Variable sflm0b and
Poping _stack by 1
ST1077a
Setting of place part of sflm0b to Local Variable place0b,
Setting of level1 part of place0b to Local Variable lev0b,
Setting of index part of place0b to Local Variable idx0b,
Setting of value part of sflm0b to Local Variable val0b
ST1078a
ST1079a
NO
Lev1b=lev0b, idx0b =
an even number and idx0b+1=idx1b?
YES
Setting of lev0b+1 to Local Variable lev_nw
ST1080a
Setting of floor(idx0b, 2) to Local Variable idx_nw
ST1081a
Setting of (lev_nw, idx_nw) to Local Variable place_nw
ST1082a
Setting of hash_comb2 (val0b, val1b) to Local Variable val_nw
ST1083a
Setting of make-stackflm (place_nw, val_nw) to
Local Variable sflm_nw
ST1084a
Pushing of stack _stack to sflm_nw
ST1085a
Performing of Late Data Setting Process REGISTER_
COMPLE_DATA with Arguments (place_nw, sflm_nw)
ST1086a
ERROR
NORMAL END

FIG. 53

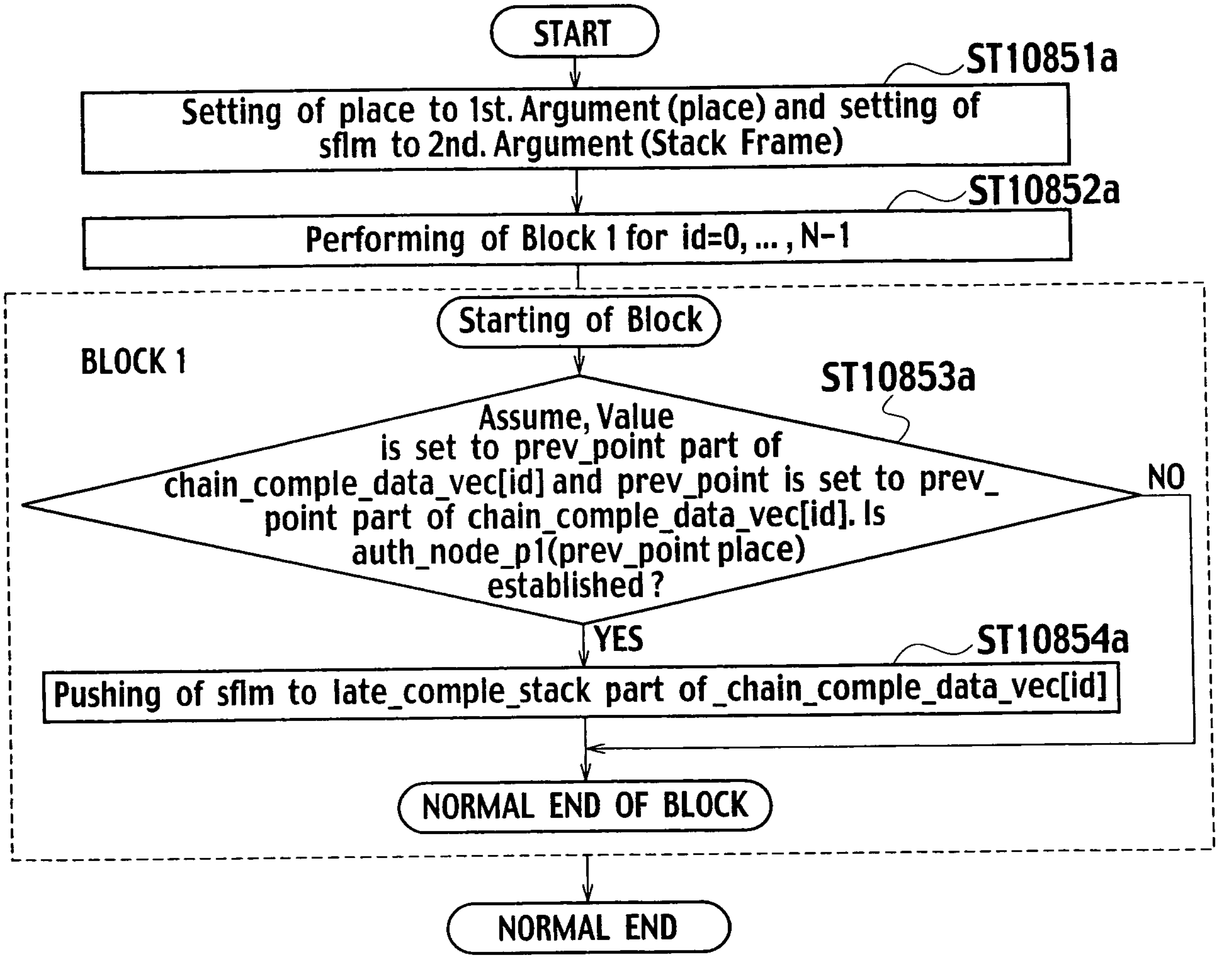

START
ST10851a
Setting of place to 1st. Argument (place) and setting of sflm to 2nd. Argument (Stack Frame)
ST10852a
Performing of Block 1 for id=0, ... , N-1
Starting of Block
BLOCK 1
ST10853a
Assume, Value is set to prev_point part of chain_comple_data_vec[id] and prev_point is set to prev_ point part of chain_comple_data_vec[id]. Is auth_node_p1(prev_point place) established ?
NO
YES
ST10854a
Pushing of sflm to late_comple_stack part of_chain_comple_data_vec[id]
NORMAL END OF BLOCK
NORMAL END

FIG. 54

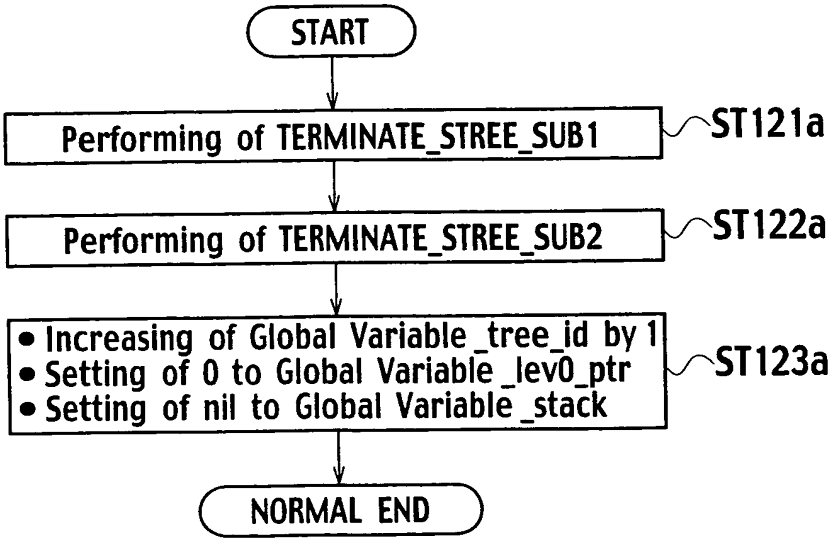

START
Performing of TERMINATE_STREE_SUB1
ST121a
Performing of TERMINATE_STREE_SUB2
ST122a
• Increasing of Global Variable _tree_id by 1
• Setting of 0 to Global Variable _lev0_ptr
• Setting of nil to Global Variable _stack
ST123a
NORMAL END

FIG. 55

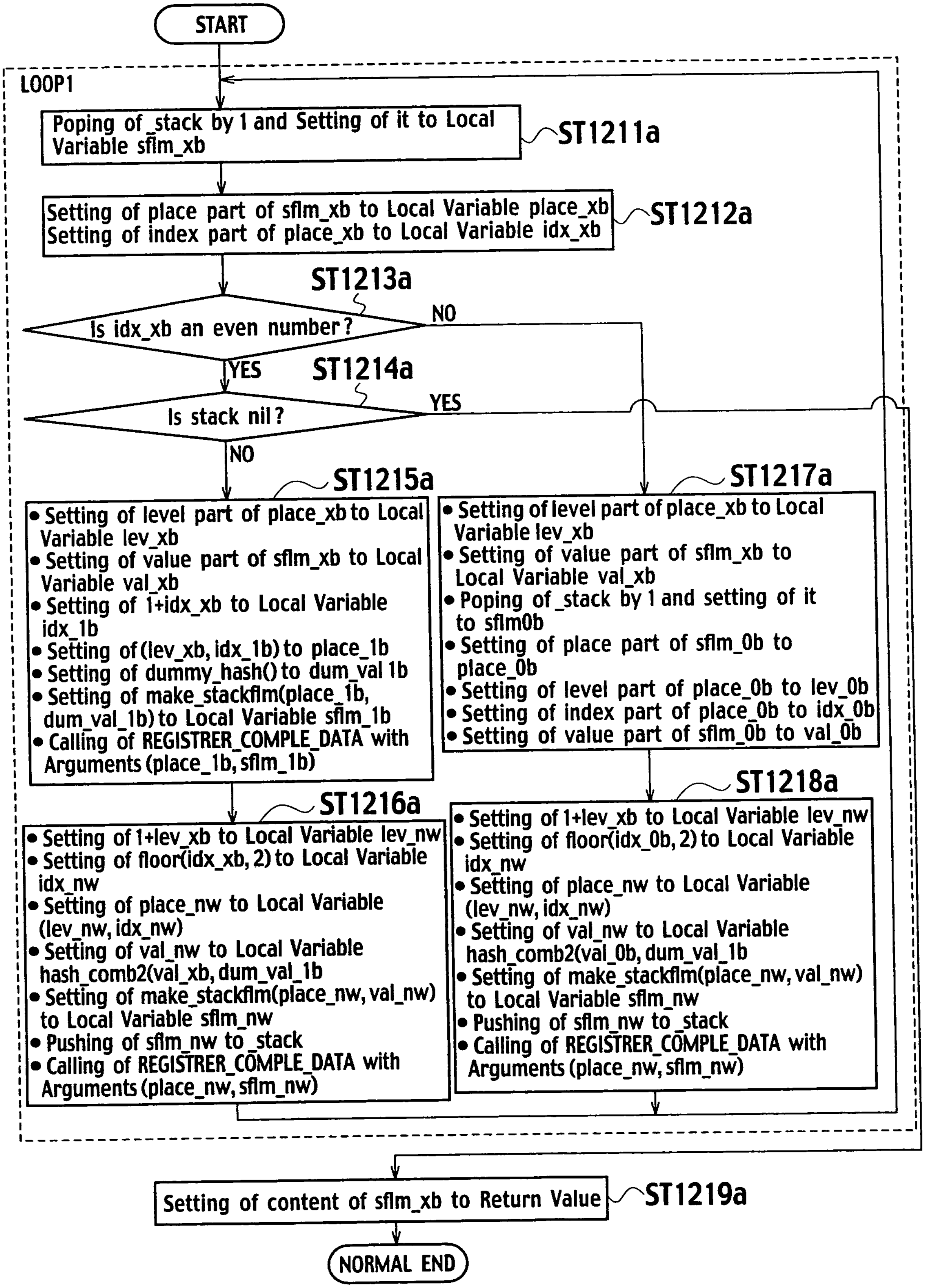

START
LOOP1
Poping of _stack by 1 and Setting of it to Local Variable sflm_xb
ST1211a
Setting of place part of sflm_xb to Local Variable place_xb
Setting of index part of place_xb to Local Variable idx_xb
ST1212a
ST1213a
Is idx_xb an even number?
NO
YES
ST1214a
Is stack nil?
YES
NO
ST1215a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sflm_xb to Local Variable val_xb
• Setting of 1+idx_xb to Local Variable idx_1b
• Setting of (lev_xb, idx_1b) to place_1b
• Setting of dummy_hash() to dum_val 1b
• Setting of make_stackflm(place_1b, dum_val_1b) to Local Variable sflm_1b
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_1b, sflm_1b)
ST1217a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sflm_xb to Local Variable val_xb
• Poping of _stack by 1 and setting of it to sflm0b
• Setting of place part of sflm_0b to place_0b
• Setting of level part of place_0b to lev_0b
• Setting of index part of place_0b to idx_0b
• Setting of value part of sflm_0b to val_0b
ST1216a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_xb, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_xb, dum_val_1b
• Setting of make_stackflm(place_nw, val_nw) to Local Variable sflm_nw
• Pushing of sflm_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sflm_nw)
ST1218a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_0b, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_0b, dum_val_1b
• Setting of make_stackflm(place_nw, val_nw) to Local Variable sflm_nw
• Pushing of sflm_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sflm_nw)
Setting of content of sflm_xb to Return Value
ST1219a
NORMAL END

FIG. 56

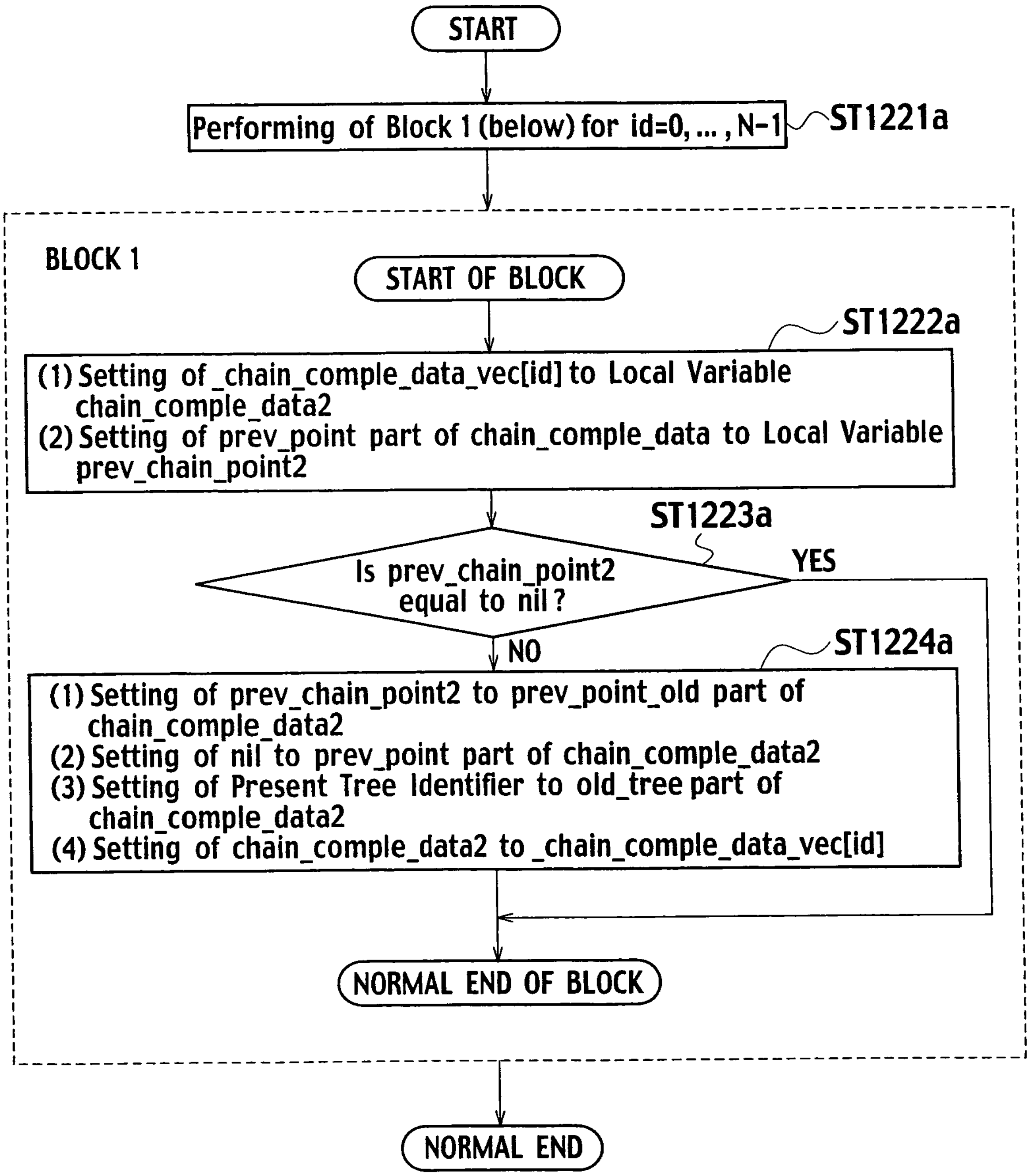

START
Performing of Block 1 (below) for id=0, ... , N-1
ST1221a
BLOCK 1
START OF BLOCK
ST1222a
(1) Setting of _chain_comple_data_vec[id] to Local Variable chain_comple_data2
(2) Setting of prev_point part of chain_comple_data to Local Variable prev_chain_point2
ST1223a
Is prev_chain_point2 equal to nil ?
YES
NO
ST1224a
(1) Setting of prev_chain_point2 to prev_point_old part of chain_comple_data2
(2) Setting of nil to prev_point part of chain_comple_data2
(3) Setting of Present Tree Identifier to old_tree part of chain_comple_data2
(4) Setting of chain_comple_data2 to _chain_comple_data_vec[id]
NORMAL END OF BLOCK
NORMAL END

FIG. 57

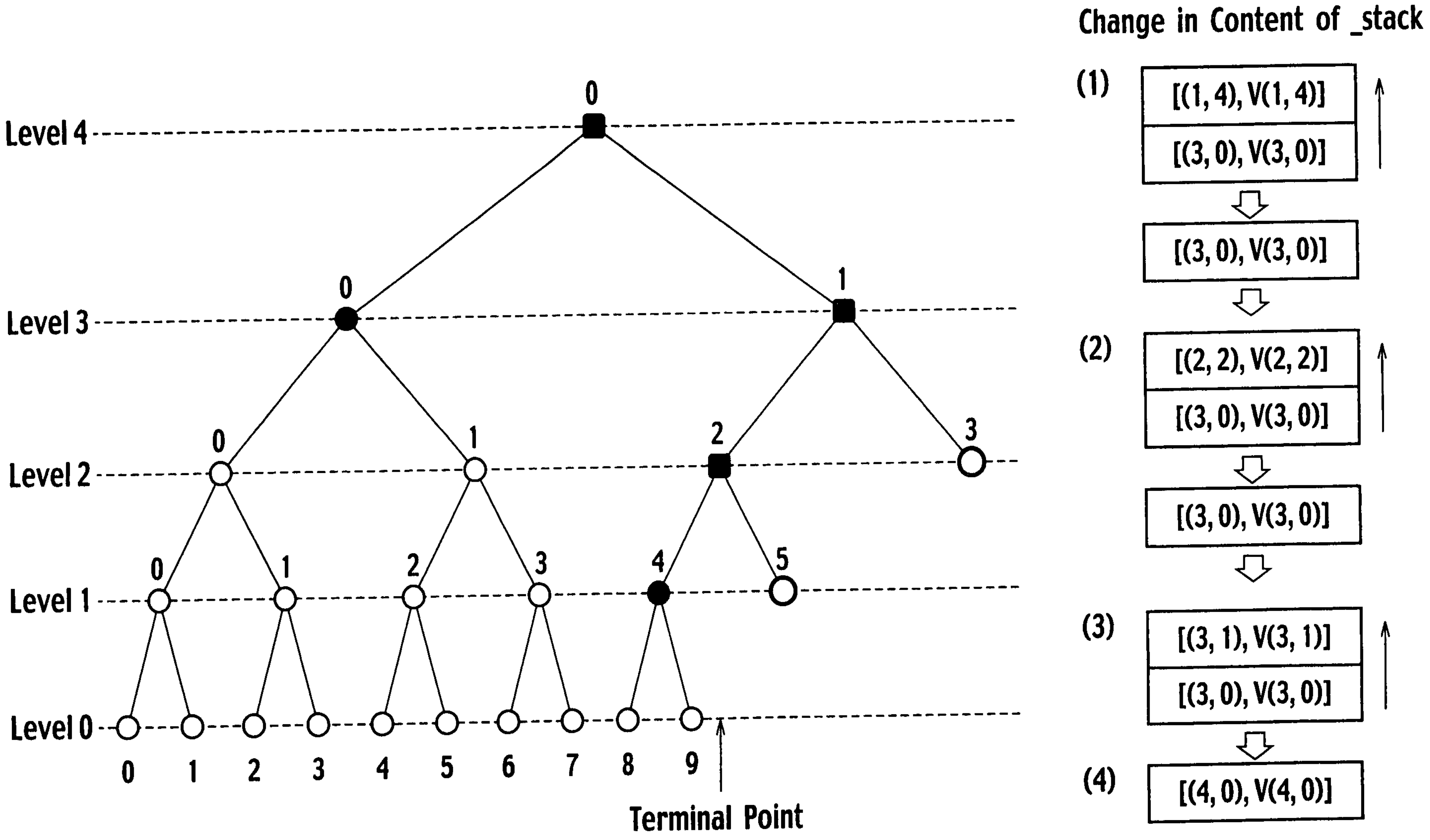
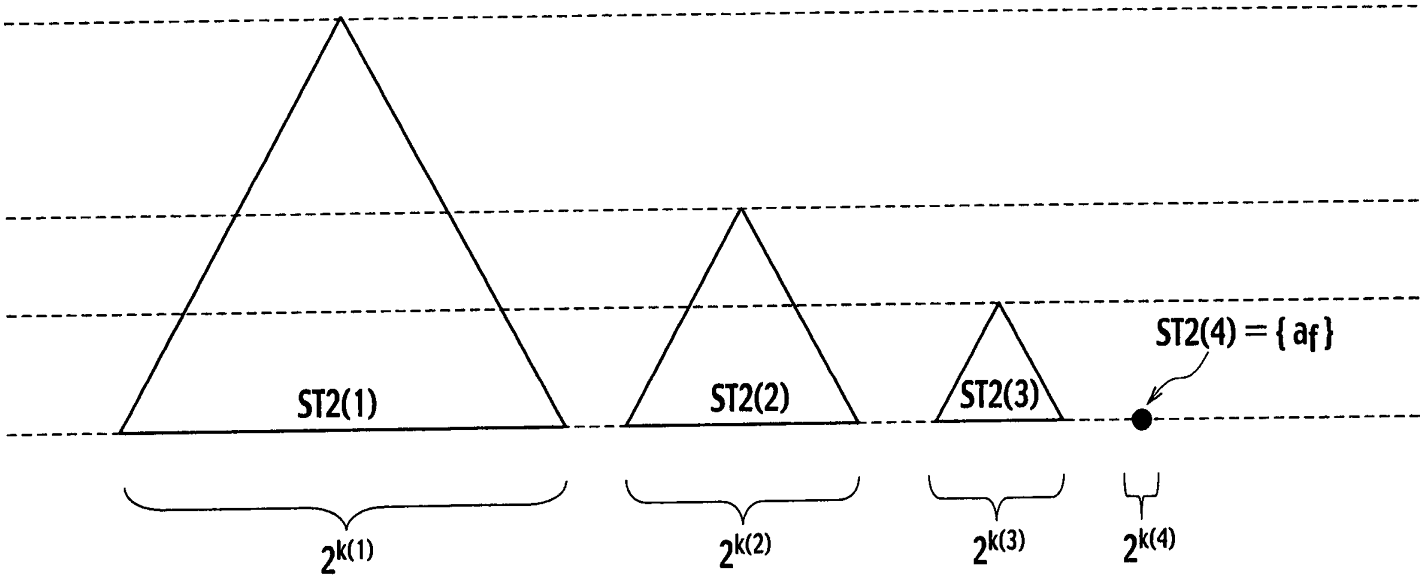

Level 4
Level 3
Level 2
Level 1
Level 0
0
0
1
0
1
2
3
0
1
2
3
4
5
0
1
2
3
4
5
6
7
8
9
Terminal Point
Change in Content of _stack
(1)
[(1, 4), V(1, 4)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(2)
[(2, 2), V(2, 2)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(3)
[(3, 1), V(3, 1)]
[(3, 0), V(3, 0)]
(4)
[(4, 0), V(4, 0)]

FIG. 58



$k(1) > k(2) > k(3) > k(4) = 0$

FIG. 59

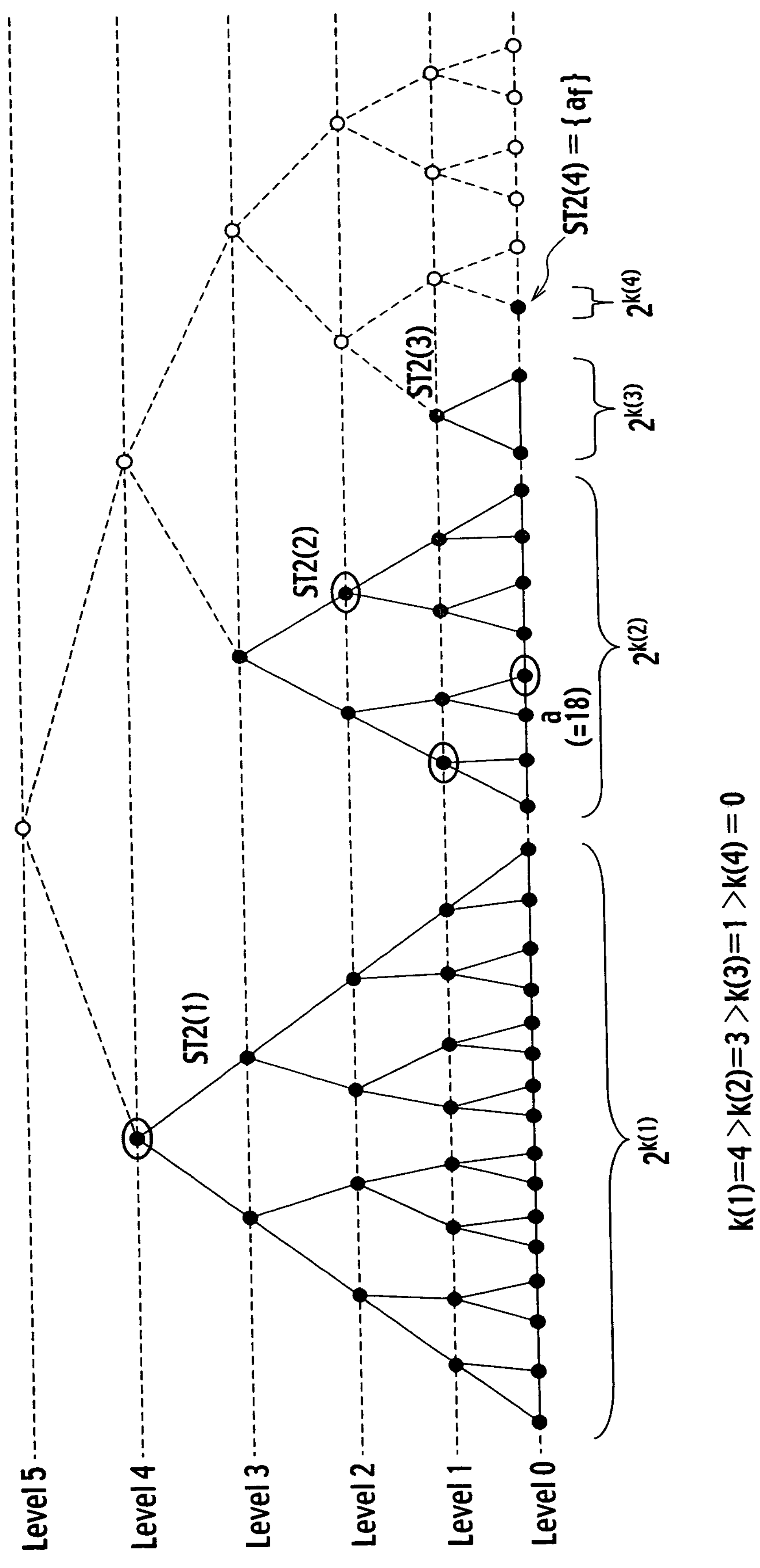

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
ST2(1)
ST2(2)
ST2(3)
ST2(4) = {af}
a
(=18)
$2^{k(1)}$
$2^{k(2)}$
$2^{k(3)}$
$2^{k(4)}$
k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0

FIG. 60

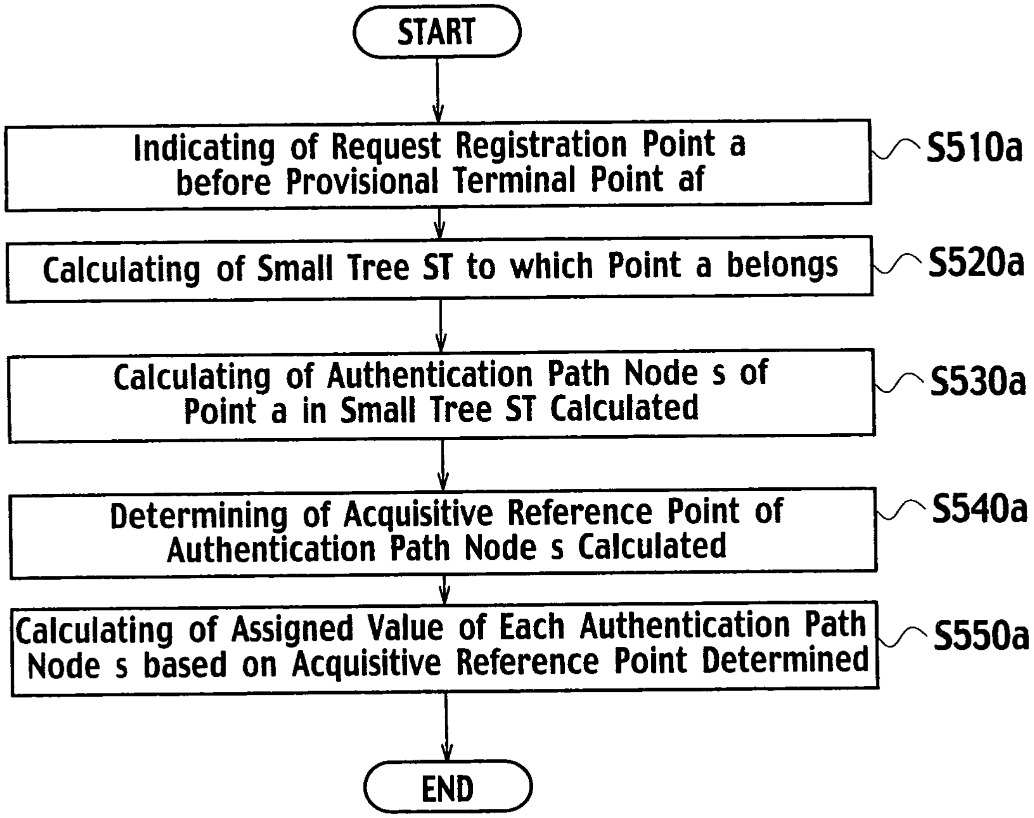
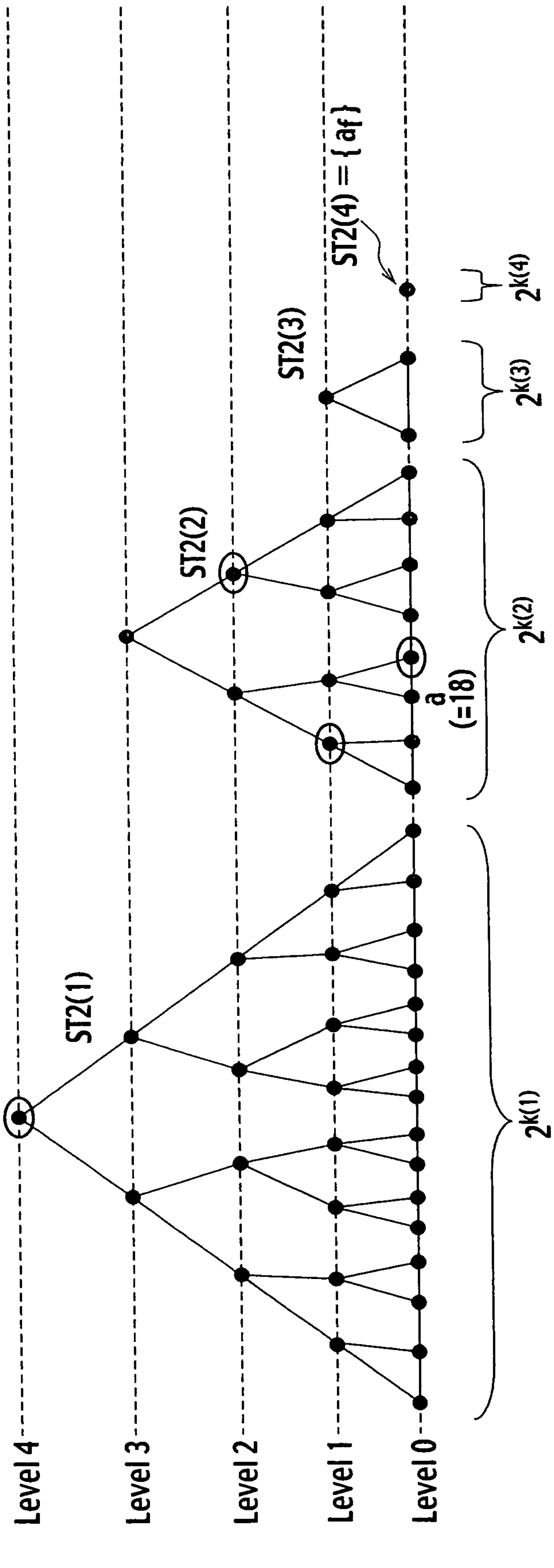

START
Indicating of Request Registration Point a before Provisional Terminal Point af
S510a
Calculating of Small Tree ST to which Point a belongs
S520a
Calculating of Authentication Path Node s of Point a in Small Tree ST Calculated
S530a
Determining of Acquisitive Reference Point of Authentication Path Node s Calculated
S540a
Calculating of Assigned Value of Each Authentication Path Node s based on Acquisitive Reference Point Determined
S550a
END

FIG. 61



$k(1)=4>k(2)=3>k(3)=1>k(4)=0$

FIG. 62

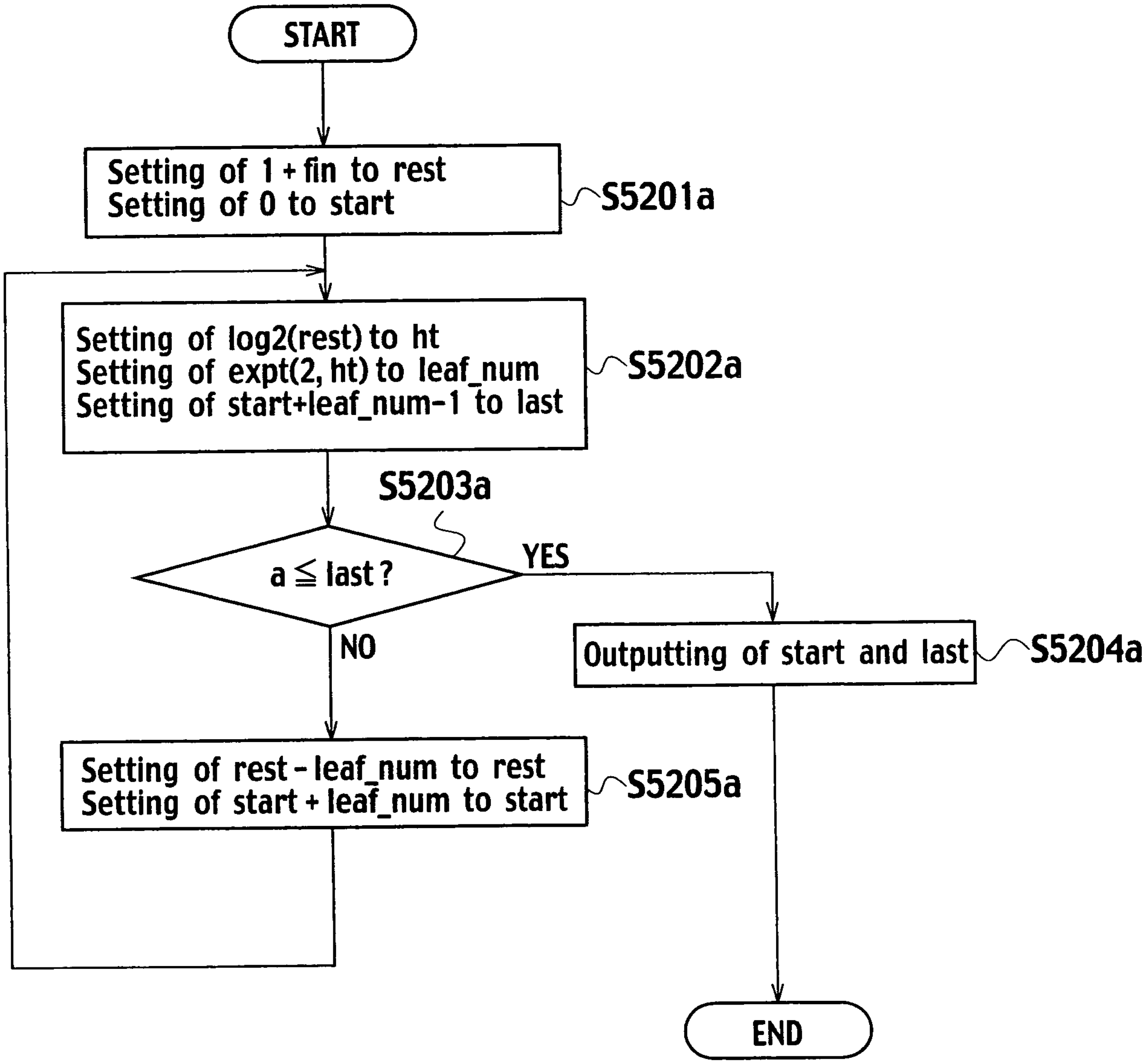

START
Setting of 1 + fin to rest
Setting of 0 to start
S5201a
Setting of log2(rest) to ht
Setting of expt(2, ht) to leaf_num
Setting of start+leaf_num-1 to last
S5202a
S5203a
a ≦ last ?
YES
NO
Outputting of start and last
S5204a
Setting of rest - leaf_num to rest
Setting of start + leaf_num to start
S5205a
END

FIG. 63

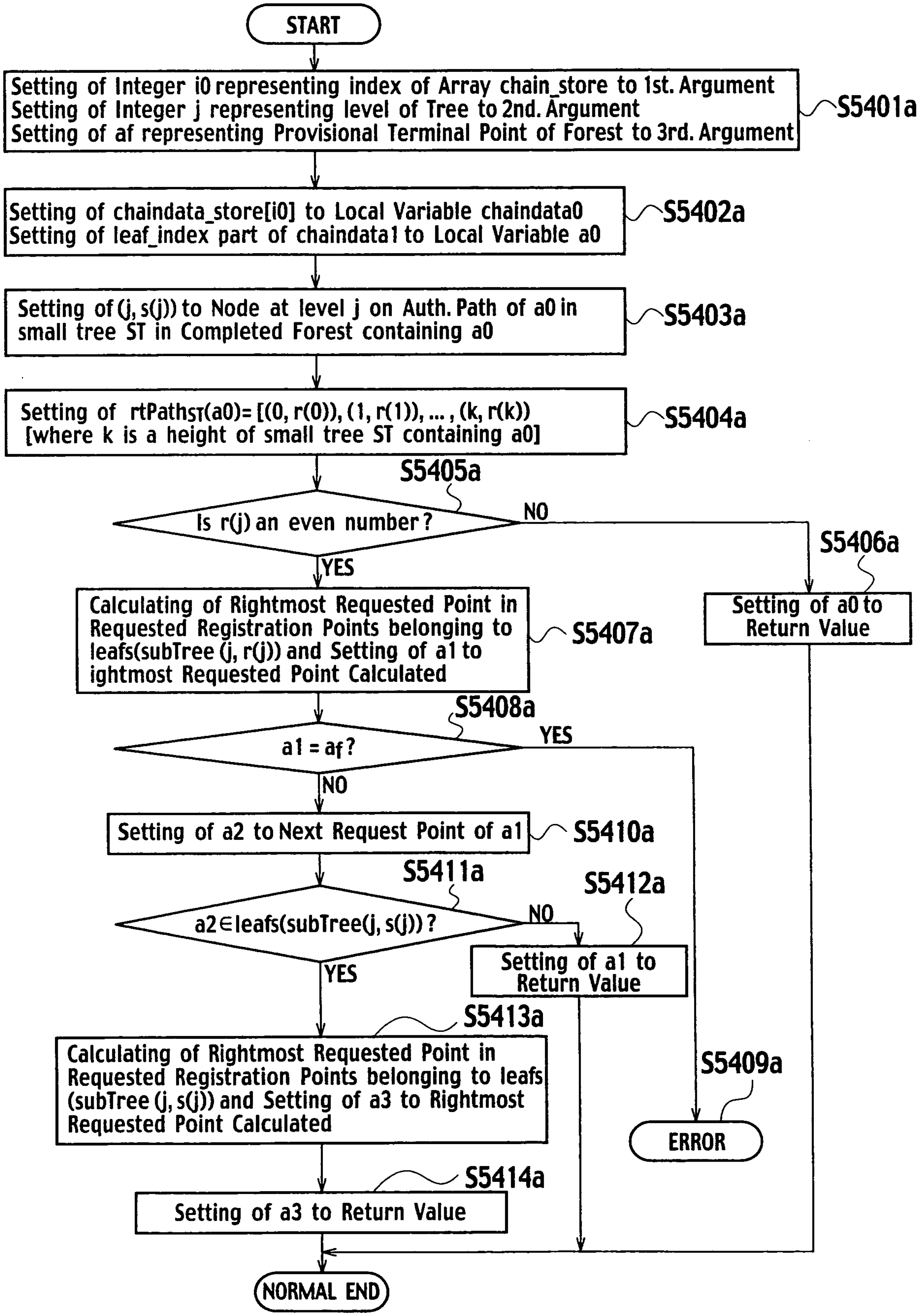

START
Setting of Integer i0 representing index of Array chain_store to 1st. Argument
Setting of Integer j representing level of Tree to 2nd. Argument
Setting of af representing Provisional Terminal Point of Forest to 3rd. Argument
S5401a
Setting of chaindata_store[i0] to Local Variable chaindata0
Setting of leaf_index part of chaindata1 to Local Variable a0
S5402a
Setting of (j, s(j)) to Node at level j on Auth. Path of a0 in small tree ST in Completed Forest containing a0
S5403a
Setting of rtPathsST(a0)= [(0, r(0)), (1, r(1)), ..., (k, r(k))
[where k is a height of small tree ST containing a0]
S5404a
S5405a
Is r(j) an even number?
NO
S5406a
Setting of a0 to Return Value
YES
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs(subTree (j, r(j)) and Setting of a1 to ightmost Requested Point Calculated
S5407a
S5408a
a1 = af?
YES
NO
Setting of a2 to Next Request Point of a1
S5410a
S5411a
S5412a
a2∈leafs(subTree(j, s(j))?
NO
Setting of a1 to Return Value
YES
S5413a
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs (subTree (j, s(j)) and Setting of a3 to Rightmost Requested Point Calculated
S5409a
ERROR
S5414a
Setting of a3 to Return Value
NORMAL END

FIG. 64

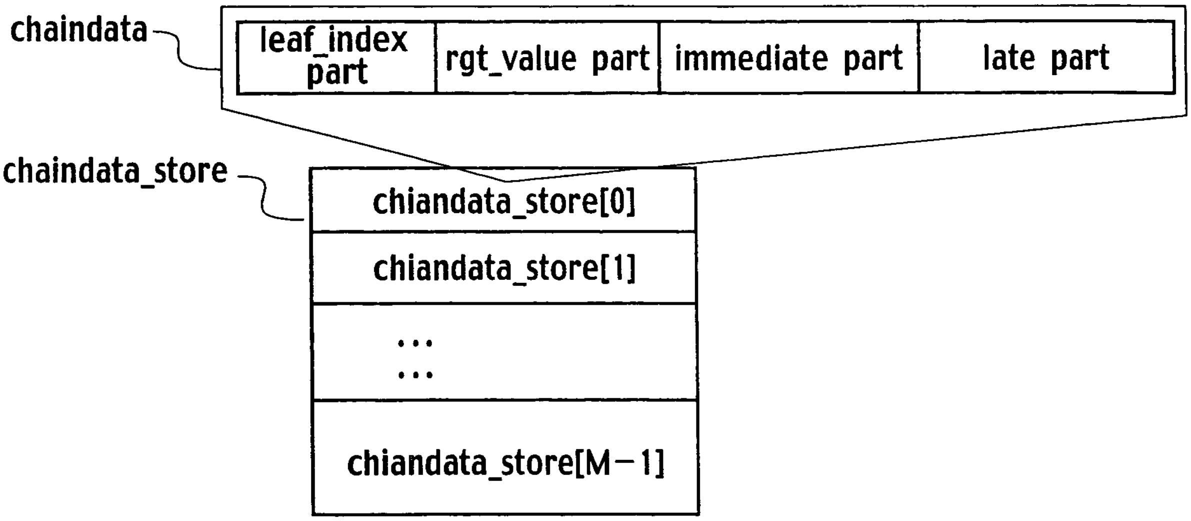

chaindata
leaf_index part
rgt_value part
immediate part
late part
chaindata_store
chiandata_store[0]
chiandata_store[1]
...
...
chiandata_store[M−1]

FIG. 65A

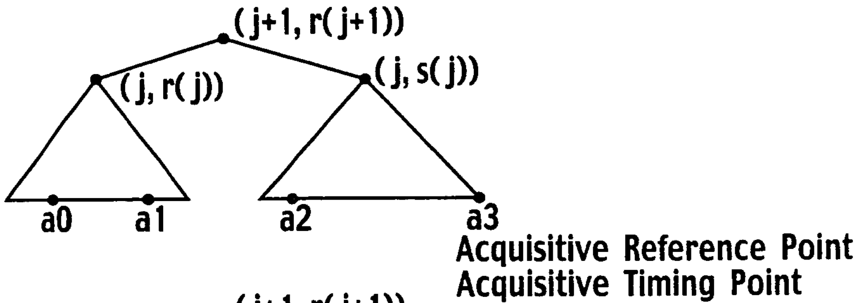


FIG. 65B

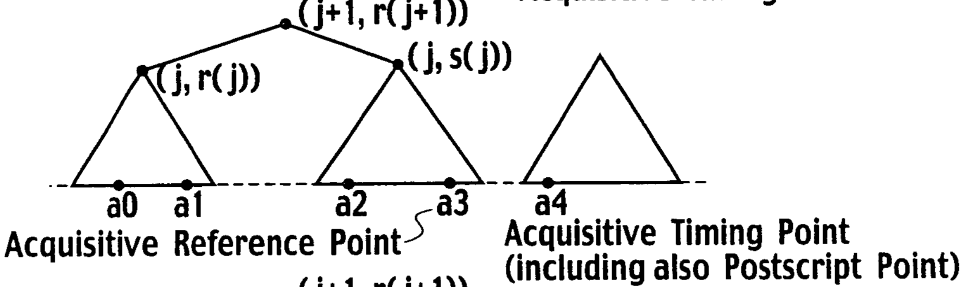


FIG. 65C

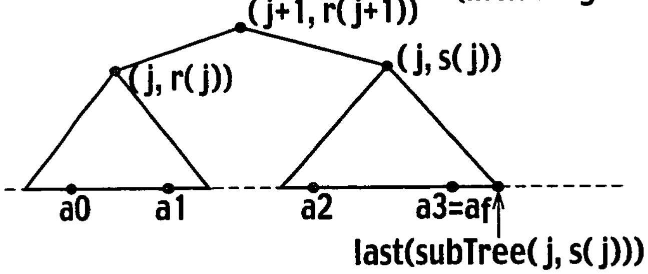


FIG. 65D

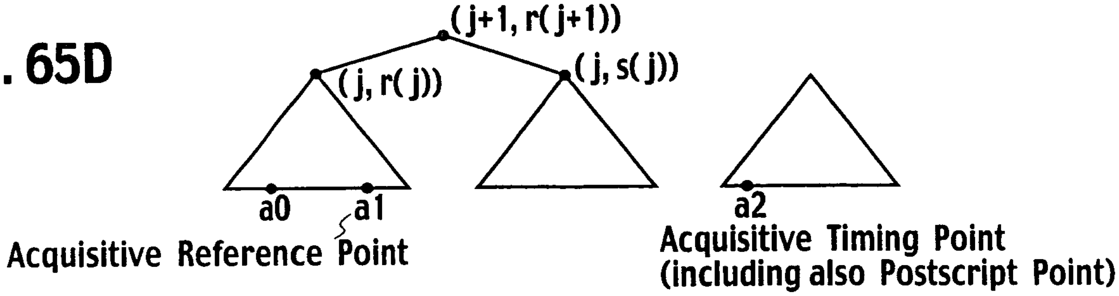


FIG. 65E

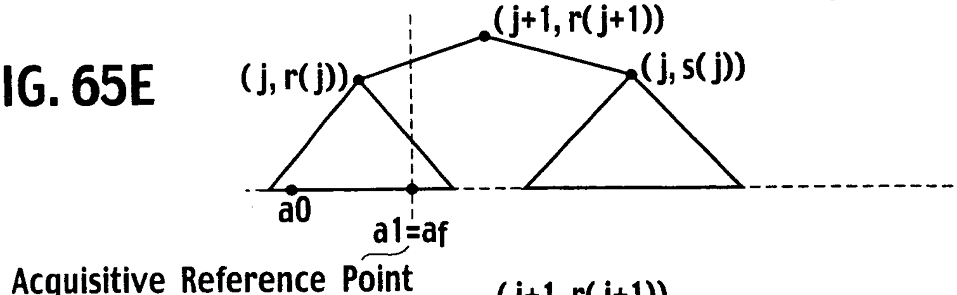


FIG. 65F

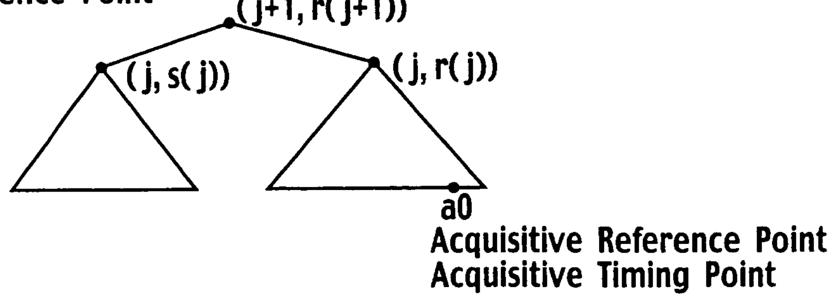


FIG. 66

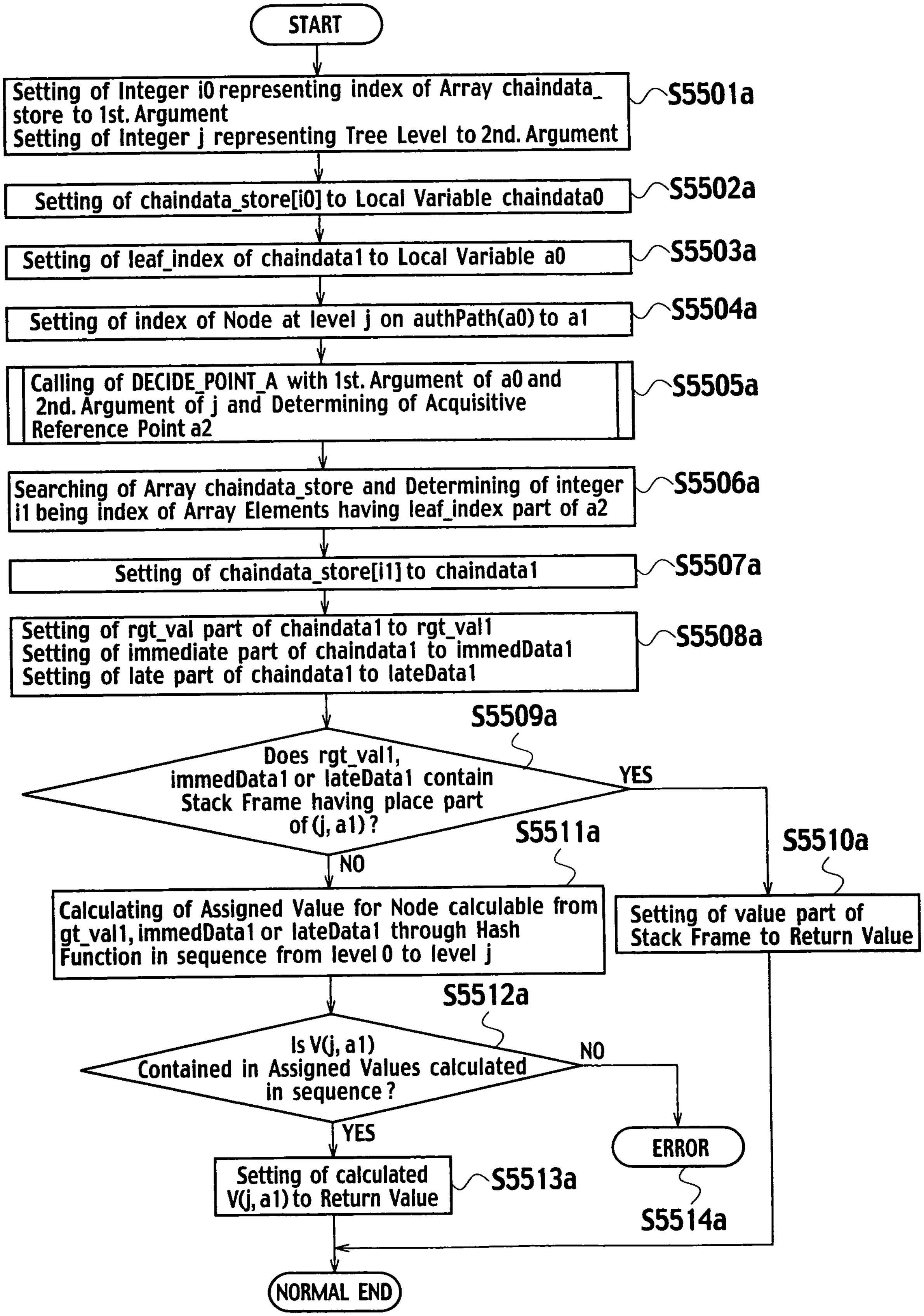

START
Setting of Integer i0 representing index of Array chaindata_store to 1st. Argument
Setting of Integer j representing Tree Level to 2nd. Argument
S5501a
Setting of chaindata_store[i0] to Local Variable chaindata0
S5502a
Setting of leaf_index of chaindata1 to Local Variable a0
S5503a
Setting of index of Node at level j on authPath(a0) to a1
S5504a
Calling of DECIDE_POINT_A with 1st. Argument of a0 and 2nd. Argument of j and Determining of Acquisitive Reference Point a2
S5505a
Searching of Array chaindata_store and Determining of integer i1 being index of Array Elements having leaf_index part of a2
S5506a
Setting of chaindata_store[i1] to chaindata1
S5507a
Setting of rgt_val part of chaindata1 to rgt_val1
Setting of immediate part of chaindata1 to immedData1
Setting of late part of chaindata1 to lateData1
S5508a
S5509a
Does rgt_val1, immedData1 or lateData1 contain Stack Frame having place part of (j, a1)?
YES
NO
S5510a
Setting of value part of Stack Frame to Return Value
S5511a
Calculating of Assigned Value for Node calculable from gt_val1, immedData1 or lateData1 through Hash Function in sequence from level 0 to level j
S5512a
Is V(j, a1) Contained in Assigned Values calculated in sequence?
NO
YES
ERROR
S5514a
Setting of calculated V(j, a1) to Return Value
S5513a
NORMAL END

FIG. 67

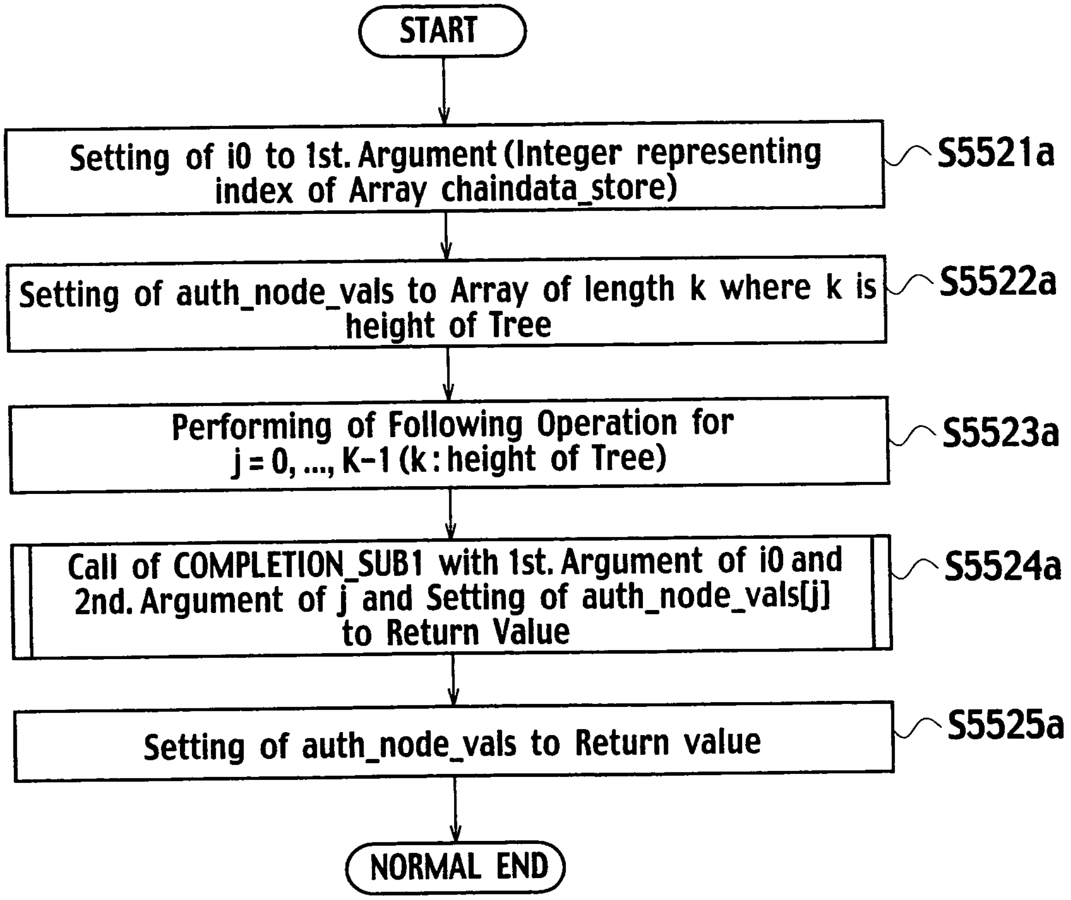

START
Setting of i0 to 1st. Argument (Integer representing index of Array chaindata_store)
S5521a
Setting of auth_node_vals to Array of length k where k is height of Tree
S5522a
Performing of Following Operation for j = 0, ..., K-1 (k: height of Tree)
S5523a
Call of COMPLETION_SUB1 with 1st. Argument of i0 and 2nd. Argument of j and Setting of auth_node_vals[j] to Return Value
S5524a
Setting of auth_node_vals to Return value
S5525a
NORMAL END

FIG. 68

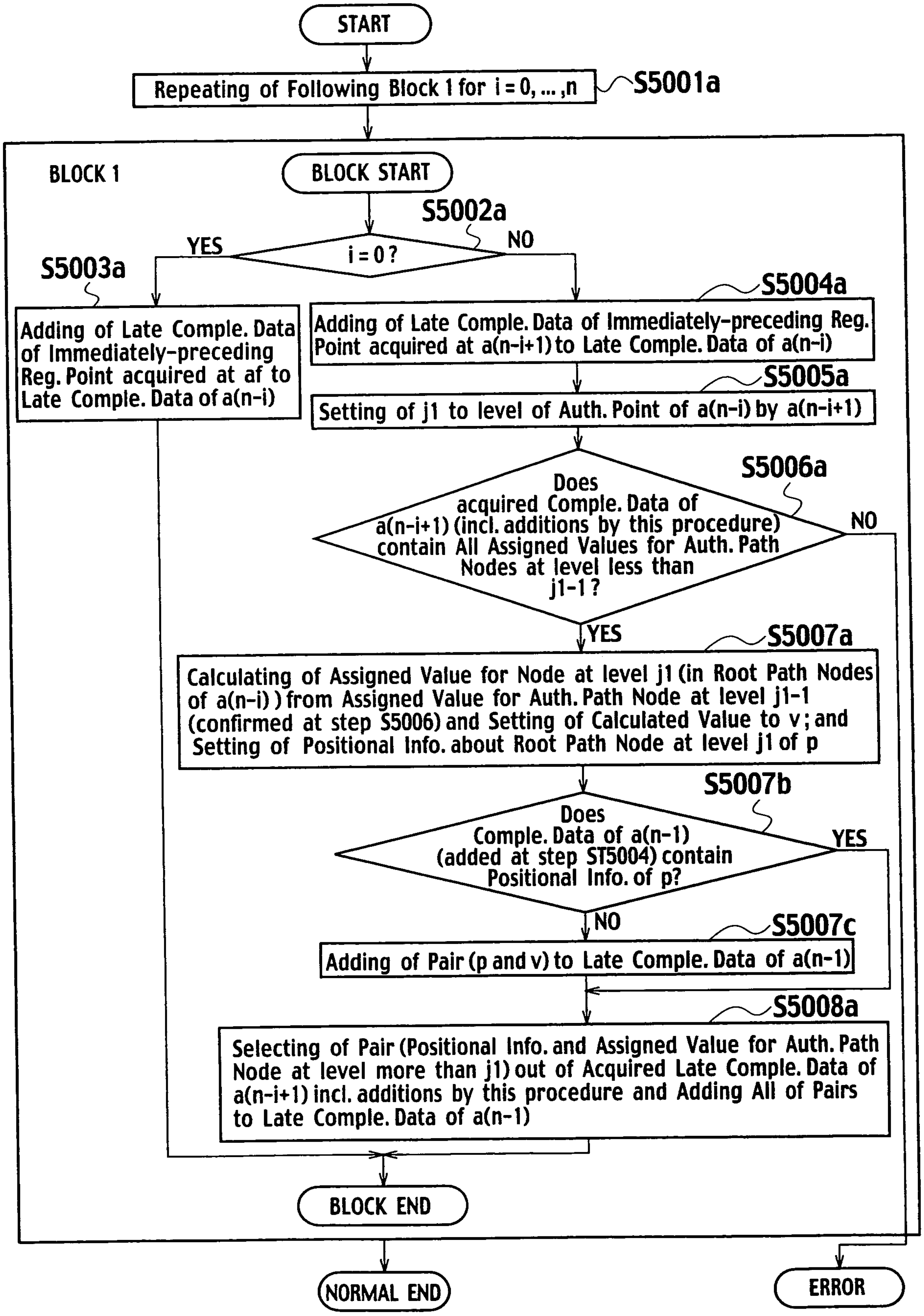

START
Repeating of Following Block 1 for i = 0, ... ,n
S5001a
BLOCK 1
BLOCK START
S5002a
i = 0 ?
YES
NO
S5003a
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at af to Late Comple. Data of a(n-i)
S5004a
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at a(n-i+1) to Late Comple. Data of a(n-i)
S5005a
Setting of j1 to level of Auth. Point of a(n-i) by a(n-i+1)
S5006a
Does acquired Comple. Data of a(n-i+1) (incl. additions by this procedure) contain All Assigned Values for Auth. Path Nodes at level less than j1-1 ?
NO
YES
S5007a
Calculating of Assigned Value for Node at level j1 (in Root Path Nodes of a(n-i)) from Assigned Value for Auth. Path Node at level j1-1 (confirmed at step S5006) and Setting of Calculated Value to v; and Setting of Positional Info. about Root Path Node at level j1 of p
S5007b
Does Comple. Data of a(n-1) (added at step ST5004) contain Positional Info. of p?
YES
NO
S5007c
Adding of Pair (p and v) to Late Comple. Data of a(n-1)
S5008a
Selecting of Pair (Positional Info. and Assigned Value for Auth. Path Node at level more than j1) out of Acquired Late Comple. Data of a(n-i+1) incl. additions by this procedure and Adding All of Pairs to Late Comple. Data of a(n-1)
BLOCK END
NORMAL END
ERROR

FIG. 69

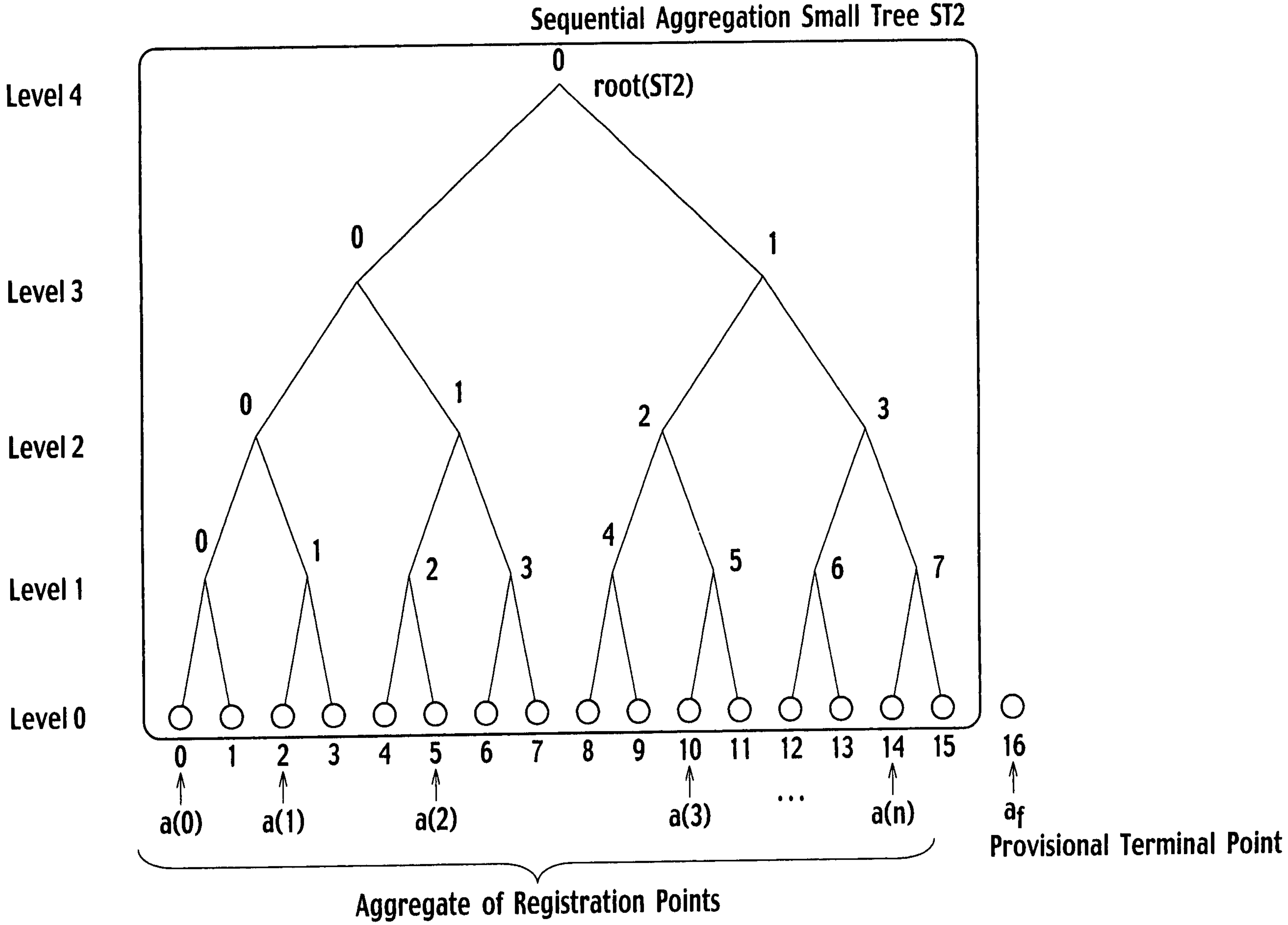

Sequential Aggregation Small Tree ST2
Level 4
Level 3
Level 2
Level 1
Level 0
0
root(ST2)
0
1
0
1
2
3
0
1
2
3
4
5
6
7
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
a(0)
a(1)
a(2)
a(3)
...
a(n)
a_f
Provisional Terminal Point
Aggregate of Registration Points

FIG. 70

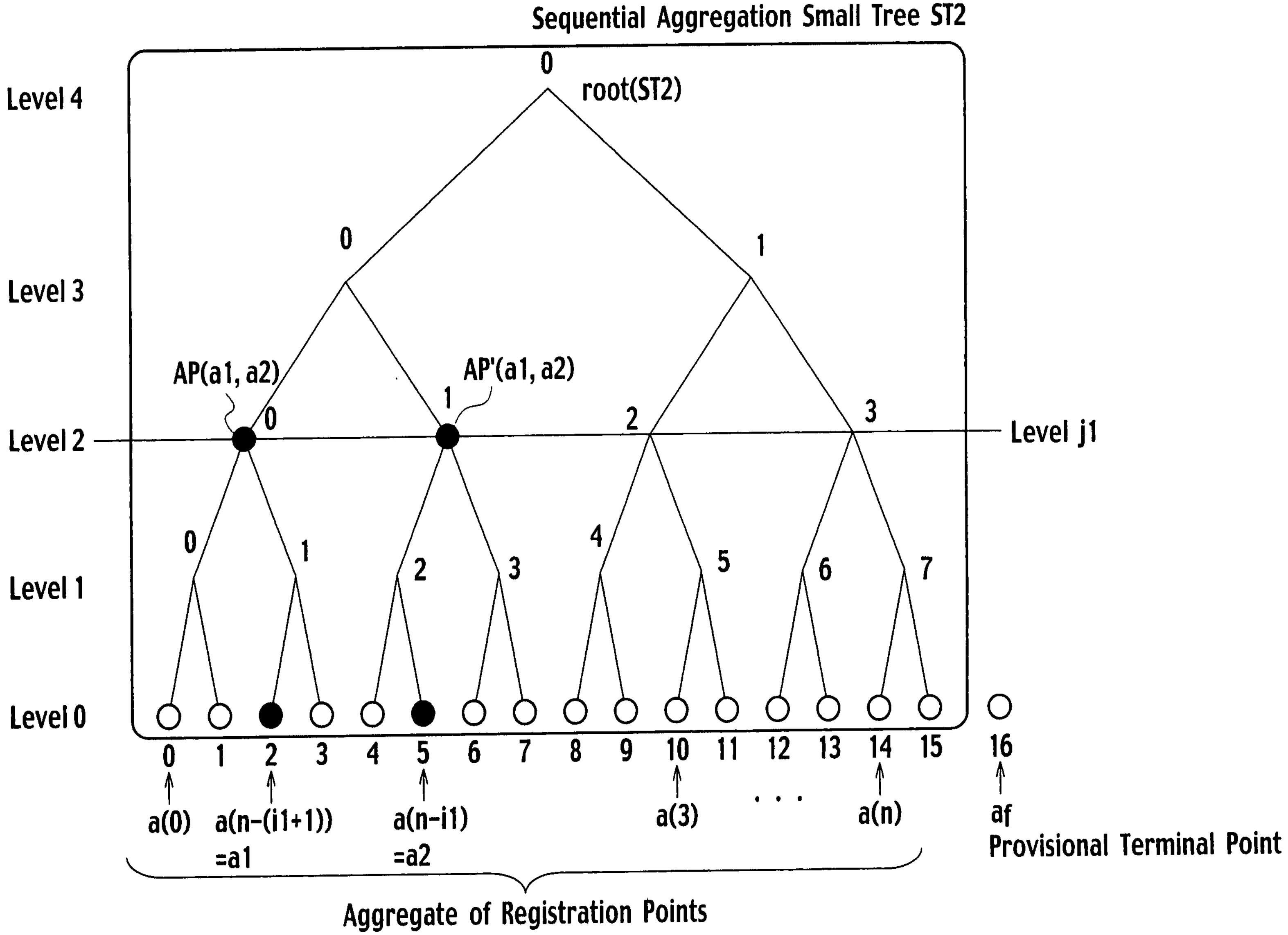
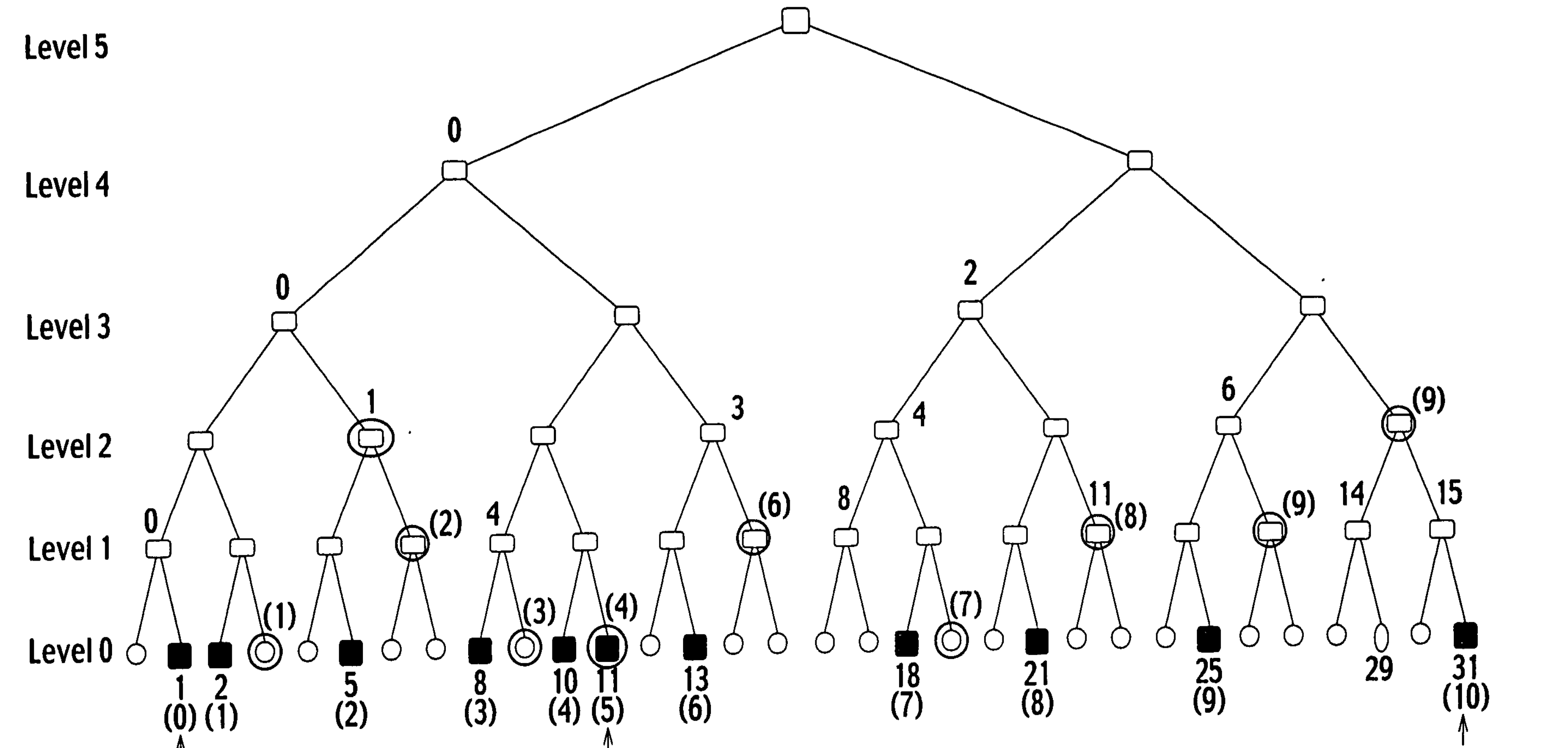
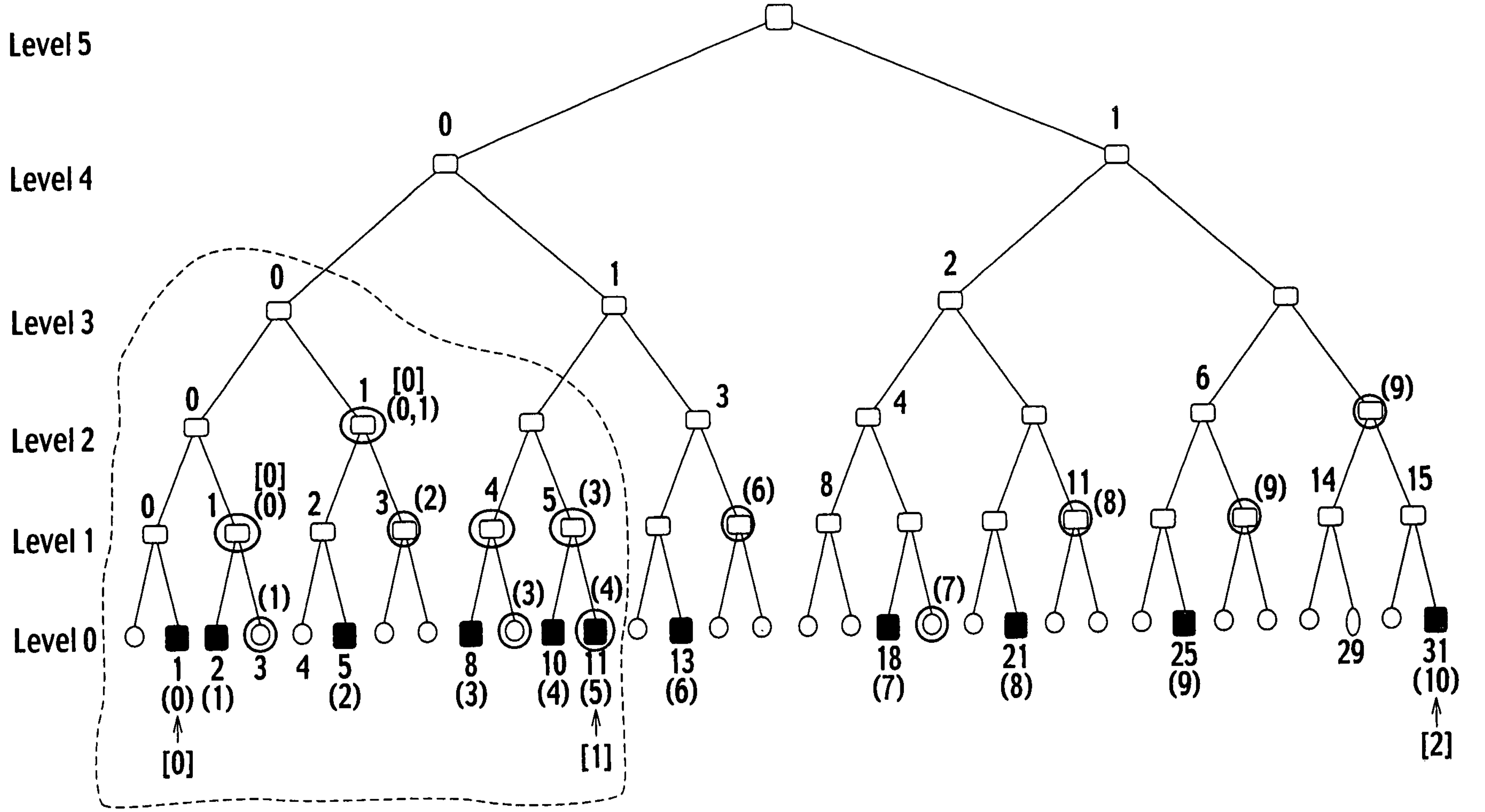

Sequential Aggregation Small Tree ST2
0
root(ST2)
Level 4
Level 3
Level 2
Level 1
Level 0
0
1
AP(a1, a2)
AP'(a1, a2)
0
1
2
3
Level j1
0
1
2
3
4
5
6
7
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
a(0)
a(n−(i1+1))
=a1
a(n−i1)
=a2
a(3)
. . .
a(n)
af
Provisional Terminal Point
Aggregate of Registration Points

FIG. 71



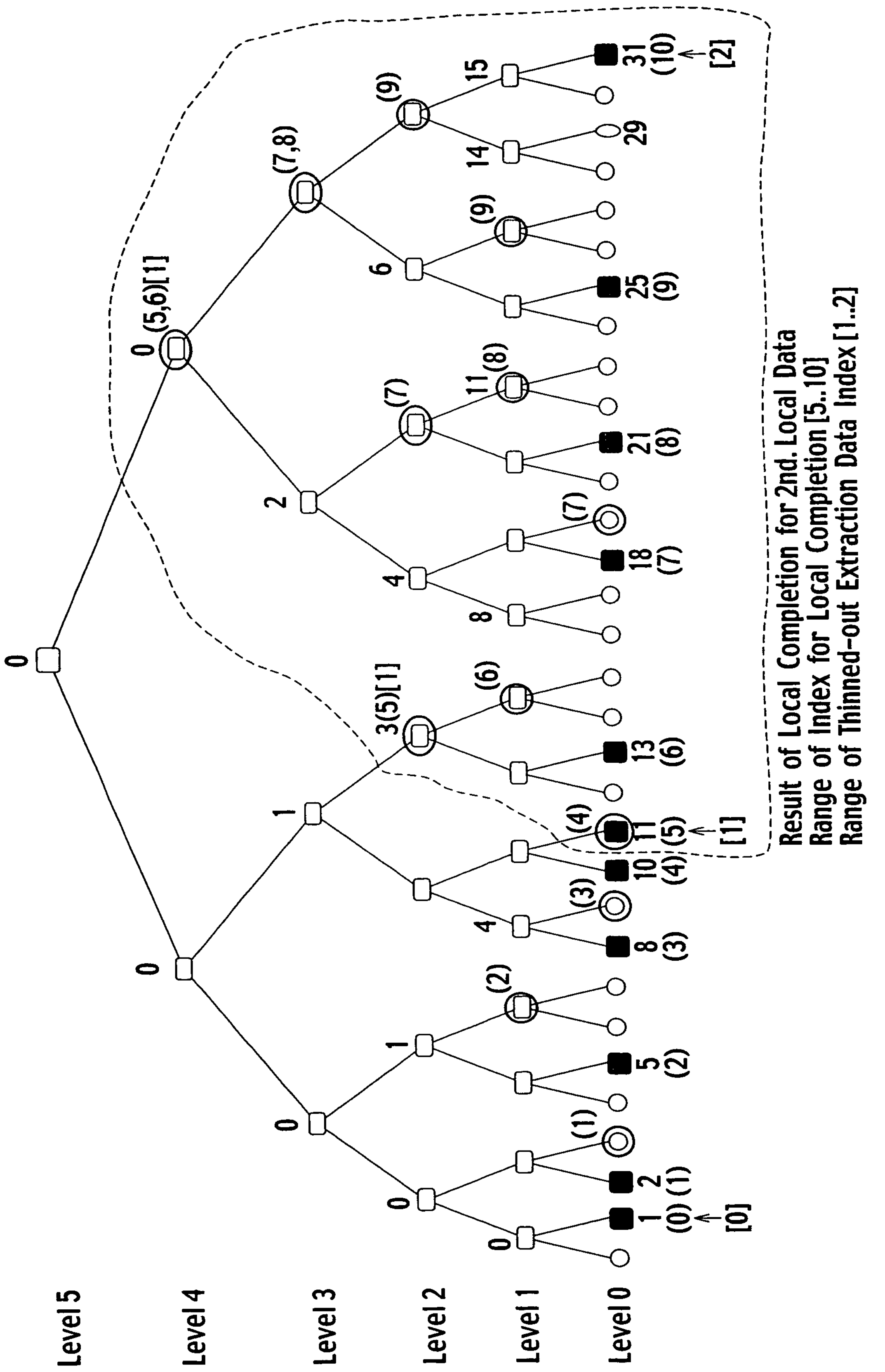
Thinned-out Extraction Data
Thinned-out Extraction Data
Setting of Thinned-out Extraction Data Index [0..2]
Thinned-out Extraction Data

FIG. 72



Result of Local Completion for 1st. Local Data
Range of Original Index for Local Completion [0..5]
Range of Thinned-out Extraction Data Index [0..1]

FIG. 73



Result of Local Completion for 2nd. Local Data
Range of Index for Local Completion [5..10]
Range of Thinned-out Extraction Data Index [1..2]

FIG. 74

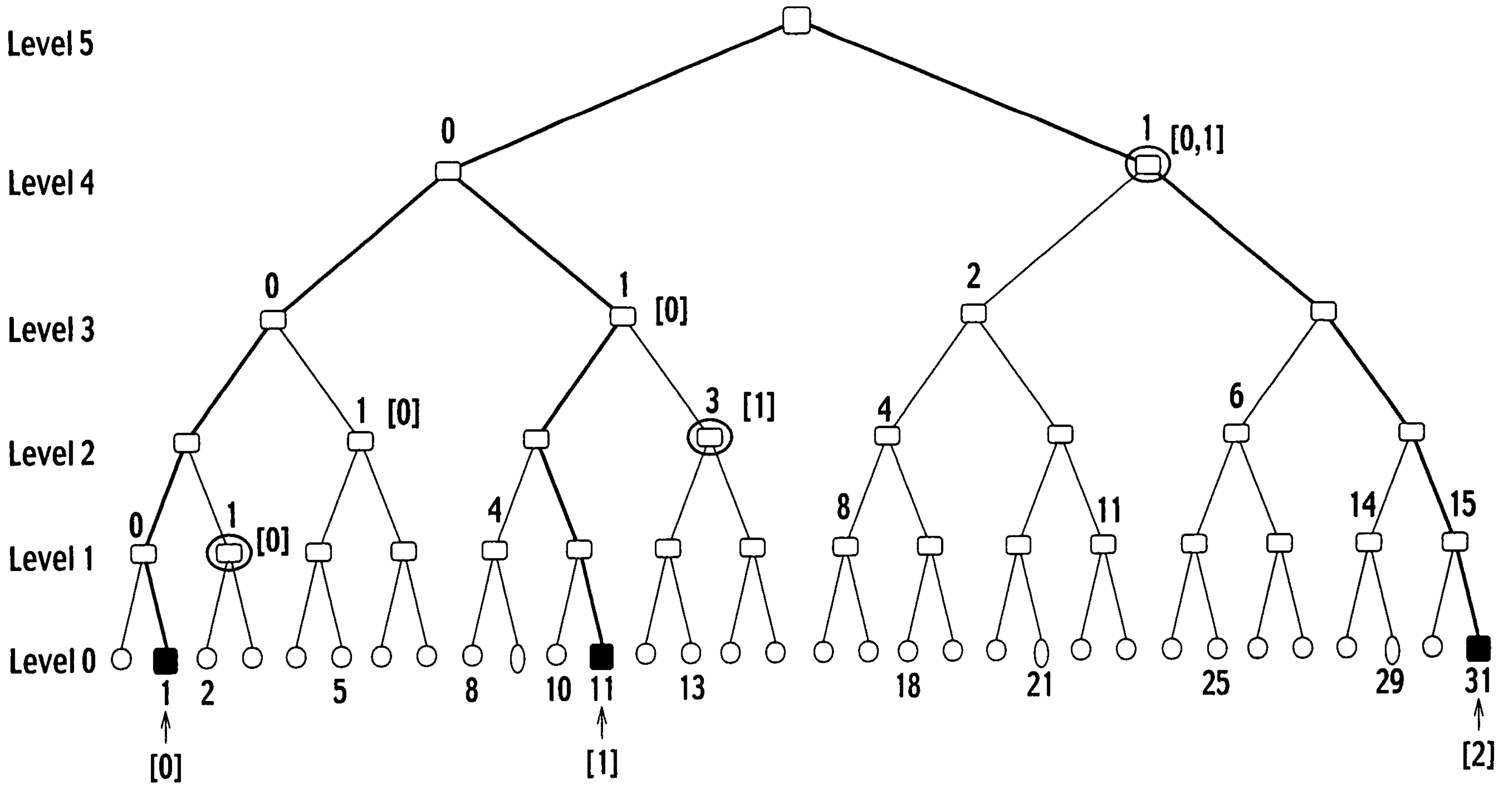

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
0
1 [0,1]
0
1 [0]
2
1 [0]
3 [1]
4
6
0
1 [0]
4
8
11
14
15
1
2
5
8
10
11
13
18
21
25
29
31
[0]
[1]
[2]

FIG. 75

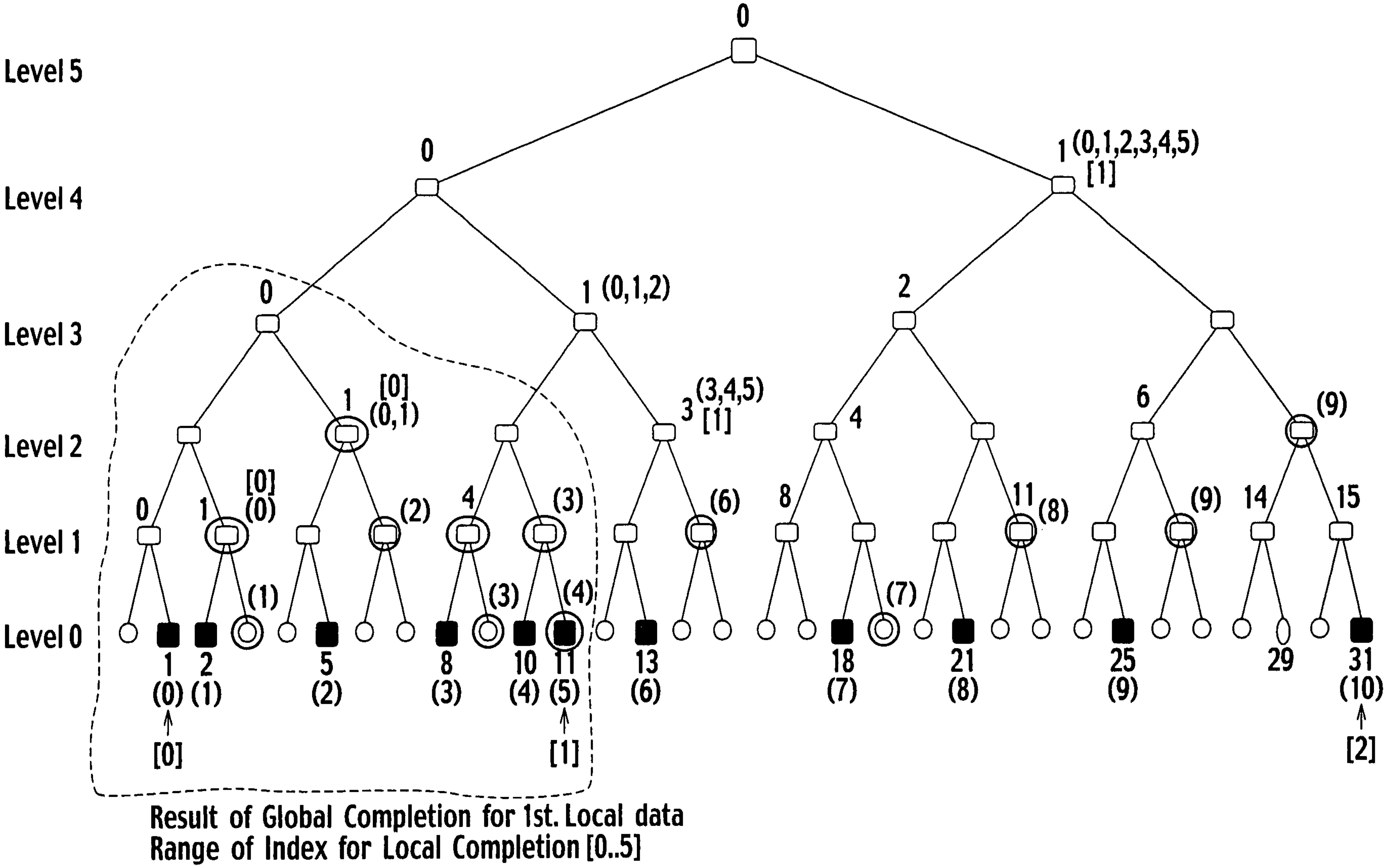

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
0
0
1 (0,1,2,3,4,5)
[1]
0
1 (0,1,2)
2
1
[0]
(0,1)
3 (3,4,5)
[1]
4
6
(9)
0
1
[0]
(0)
(2)
4
(3)
(6)
8
11 (8)
(9)
14
15
(1)
(3)
(4)
(7)
1
(0)
[0]
2
(1)
5
(2)
8
(3)
10
(4)
11
(5)
[1]
13
(6)
18
(7)
21
(8)
25
(9)
29
31
(10)
[2]
Result of Global Completion for 1st. Local data
Range of Index for Local Completion [0..5]

FIG. 76

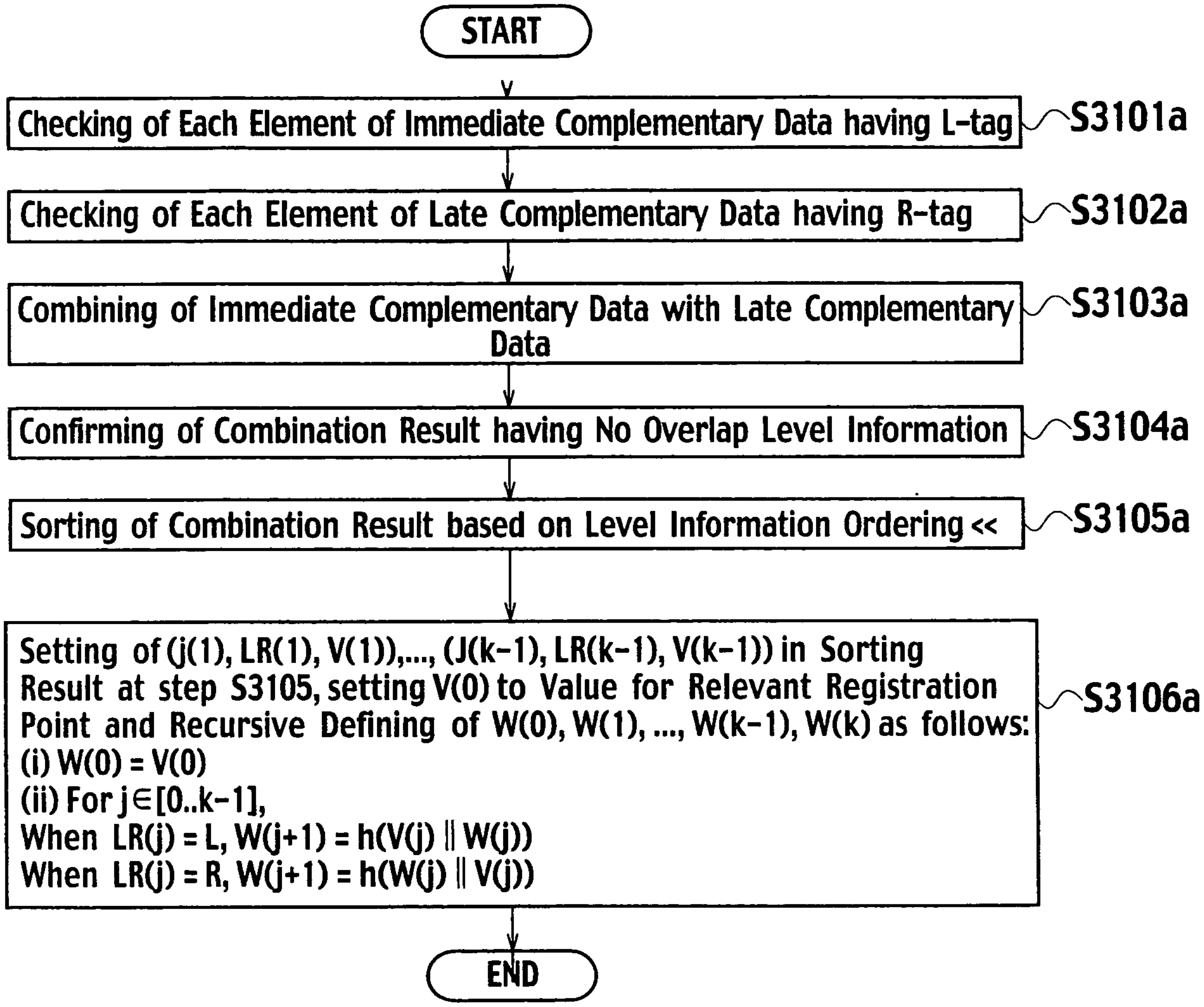
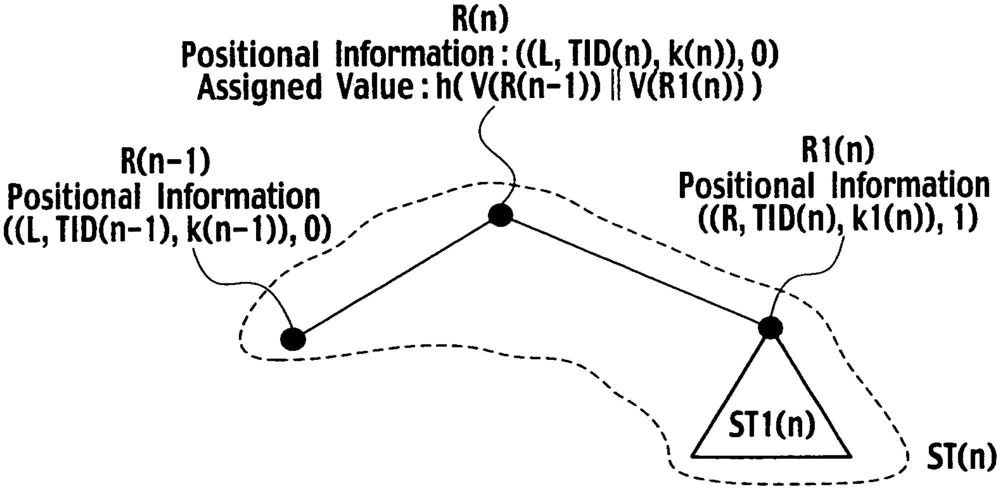

START
Checking of Each Element of Immediate Complementary Data having L-tag
S3101a
Checking of Each Element of Late Complementary Data having R-tag
S3102a
Combining of Immediate Complementary Data with Late Complementary Data
S3103a
Confirming of Combination Result having No Overlap Level Information
S3104a
Sorting of Combination Result based on Level Information Ordering <<
S3105a
Setting of (j(1), LR(1), V(1)),..., (J(k-1), LR(k-1), V(k-1)) in Sorting Result at step S3105, setting V(0) to Value for Relevant Registration Point and Recursive Defining of W(0), W(1), ..., W(k-1), W(k) as follows:
(i) W(0) = V(0)
(ii) For j∈[0..k-1],
When LR(j) = L, W(j+1) = h(V(j) || W(j))
When LR(j) = R, W(j+1) = h(W(j) || V(j))
S3106a
END

FIG. 77


R(n)
Positional Information : ((L, TID(n), k(n)), 0)
Assigned Value : h(V(R(n-1)) || V(R1(n)))
R(n-1)
Positional Information
((L, TID(n-1), k(n-1)), 0)
R1(n)
Positional Information
((R, TID(n), k1(n)), 1)
ST1(n)
ST(n)

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 71 of 77

FIG. 78

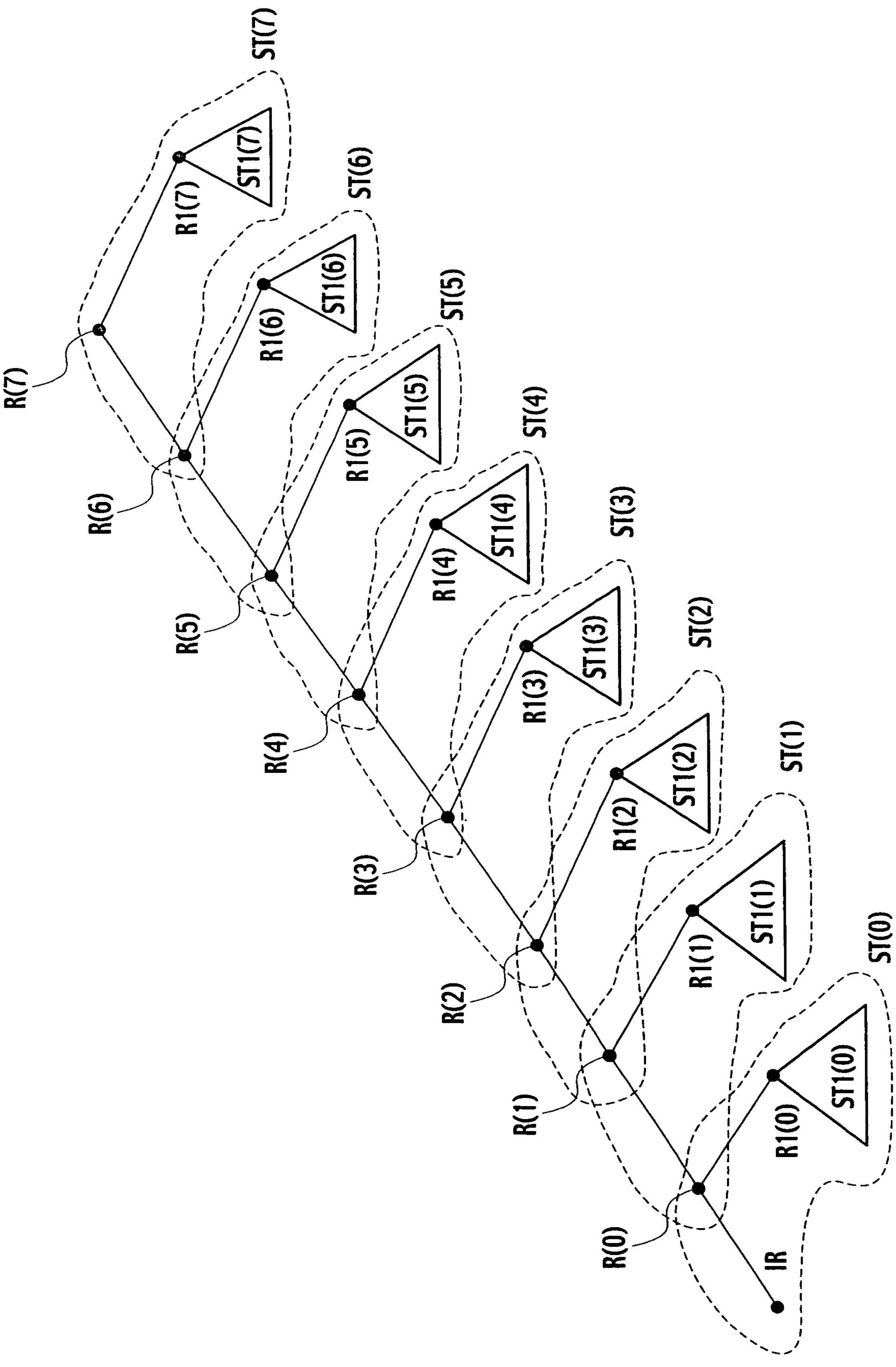


FIG. 79

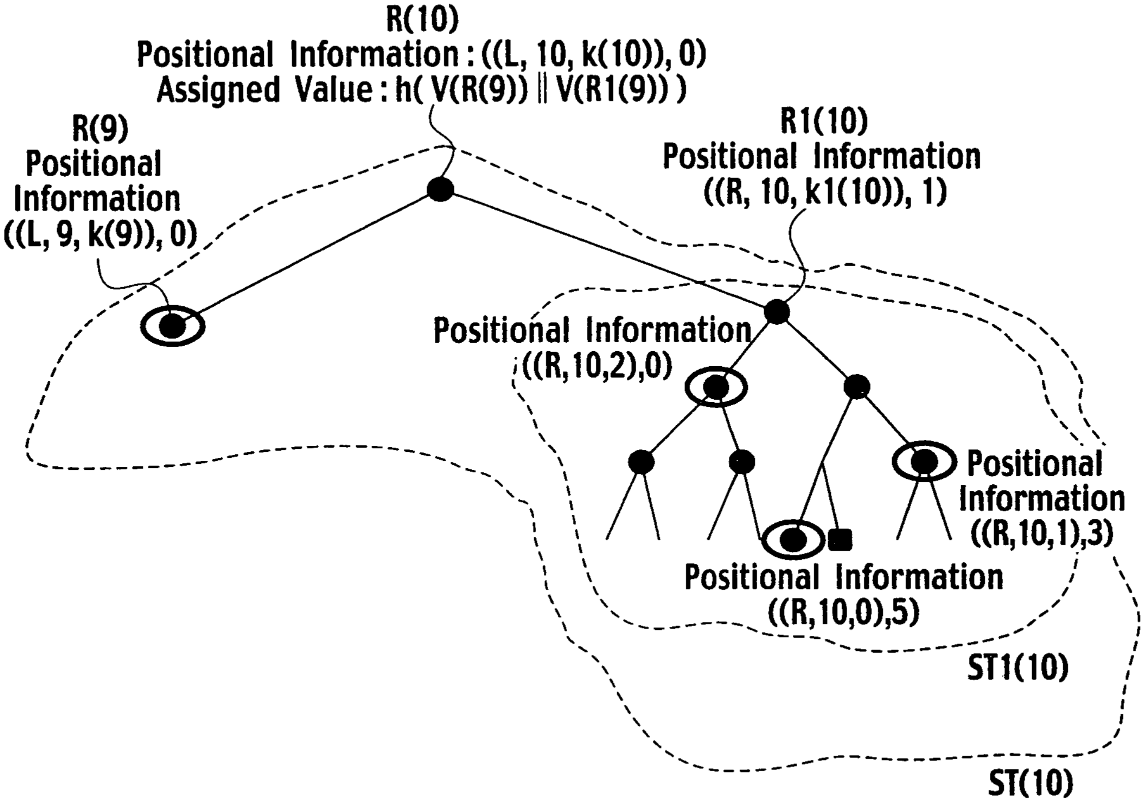

R(10)
Positional Information : ((L, 10, k(10)), 0)
Assigned Value : h(V(R(9)) || V(R1(9)))
R(9)
Positional Information
((L, 9, k(9)), 0)
R1(10)
Positional Information
((R, 10, k1(10)), 1)
Positional Information
((R,10,2),0)
Positional Information
((R,10,1),3)
Positional Information
((R,10,0),5)
ST1(10)
ST(10)

FIG. 80

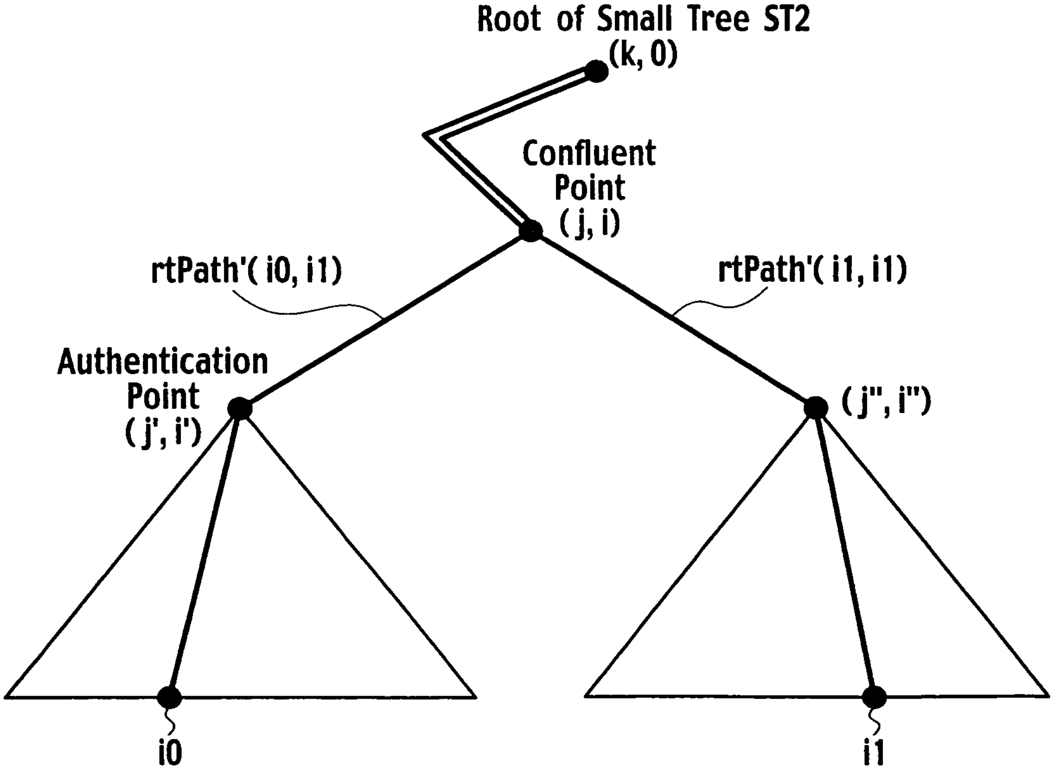

Root of Small Tree ST2
(k, 0)
Confluent Point
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
(j", i")
i0
i1

FIG. 81

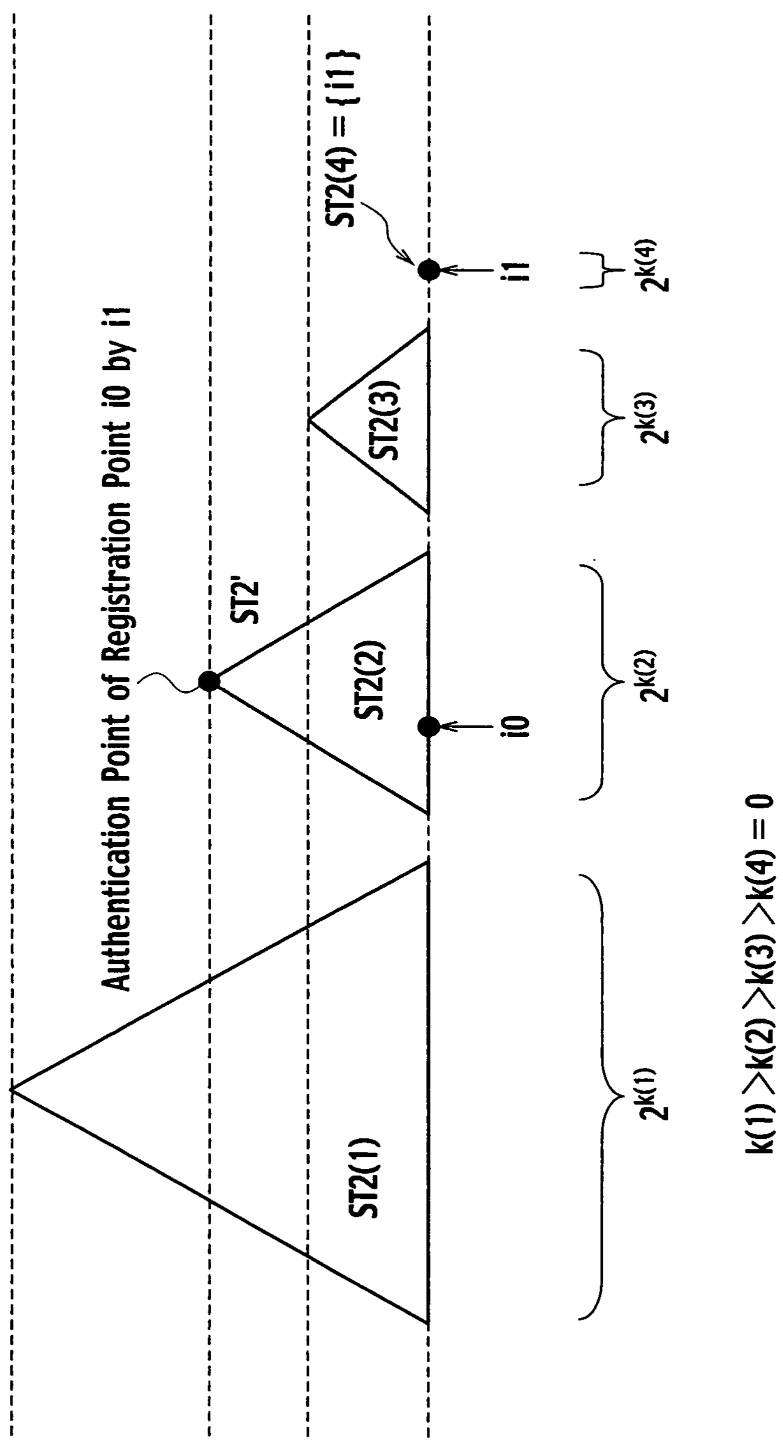

Authentication Point of Registration Point i0 by i1
ST2'
ST2(4) = {i1}
ST2(1)
ST2(2)
ST2(3)
i0
i1
$2^{k(1)}$
$2^{k(2)}$
$2^{k(3)}$
$2^{k(4)}$
k(1) > k(2) > k(3) > k(4) = 0

FIG. 82

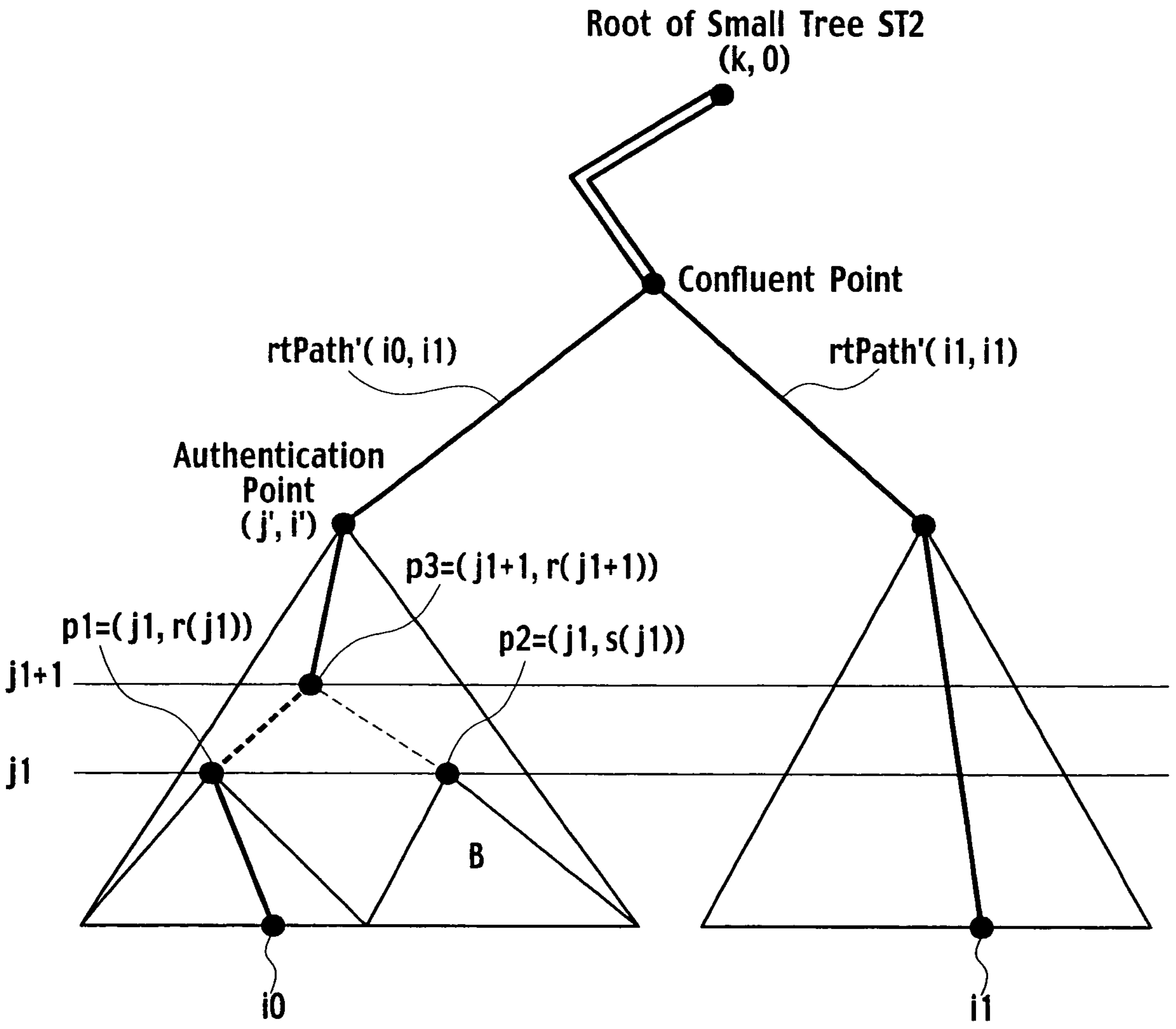

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

FIG. 83

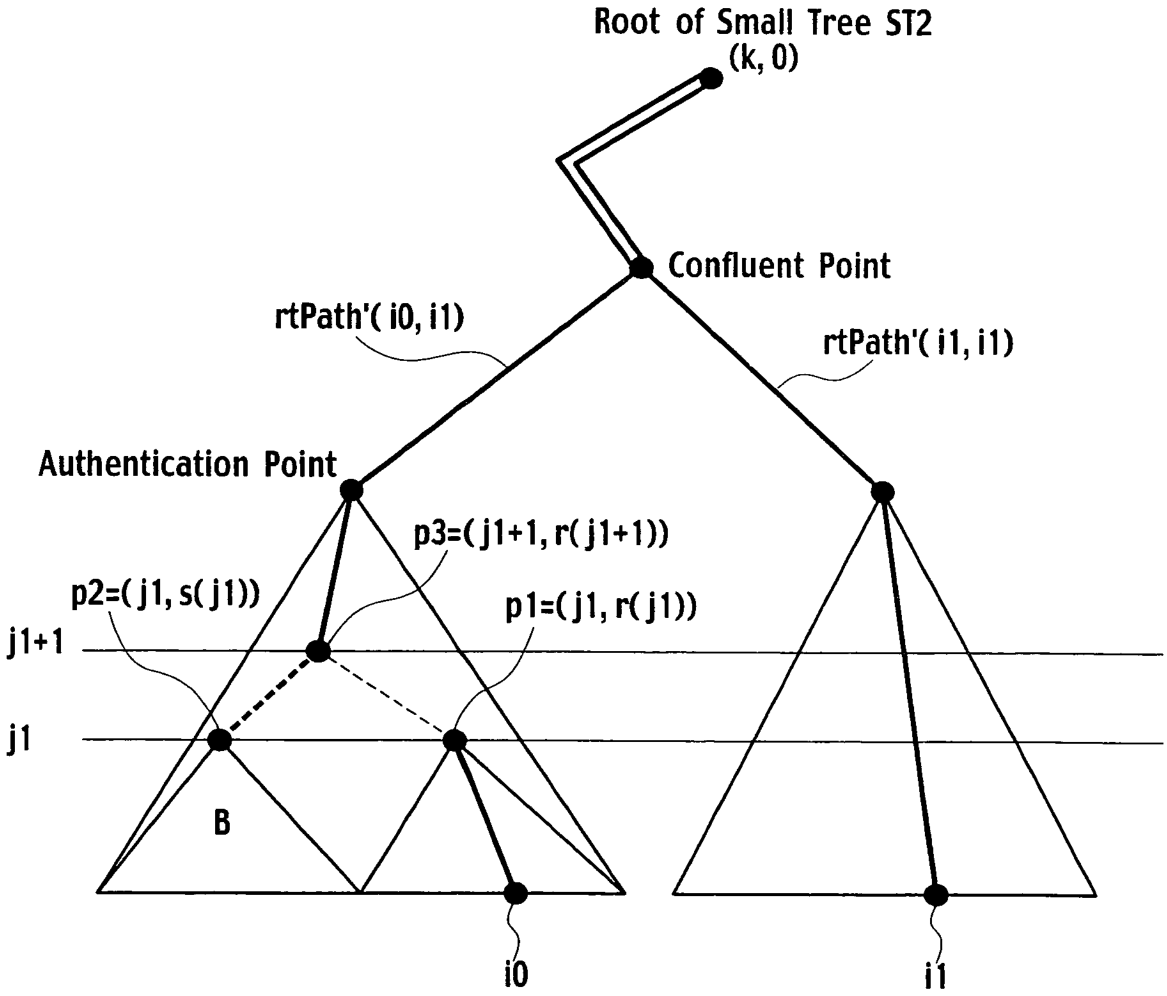
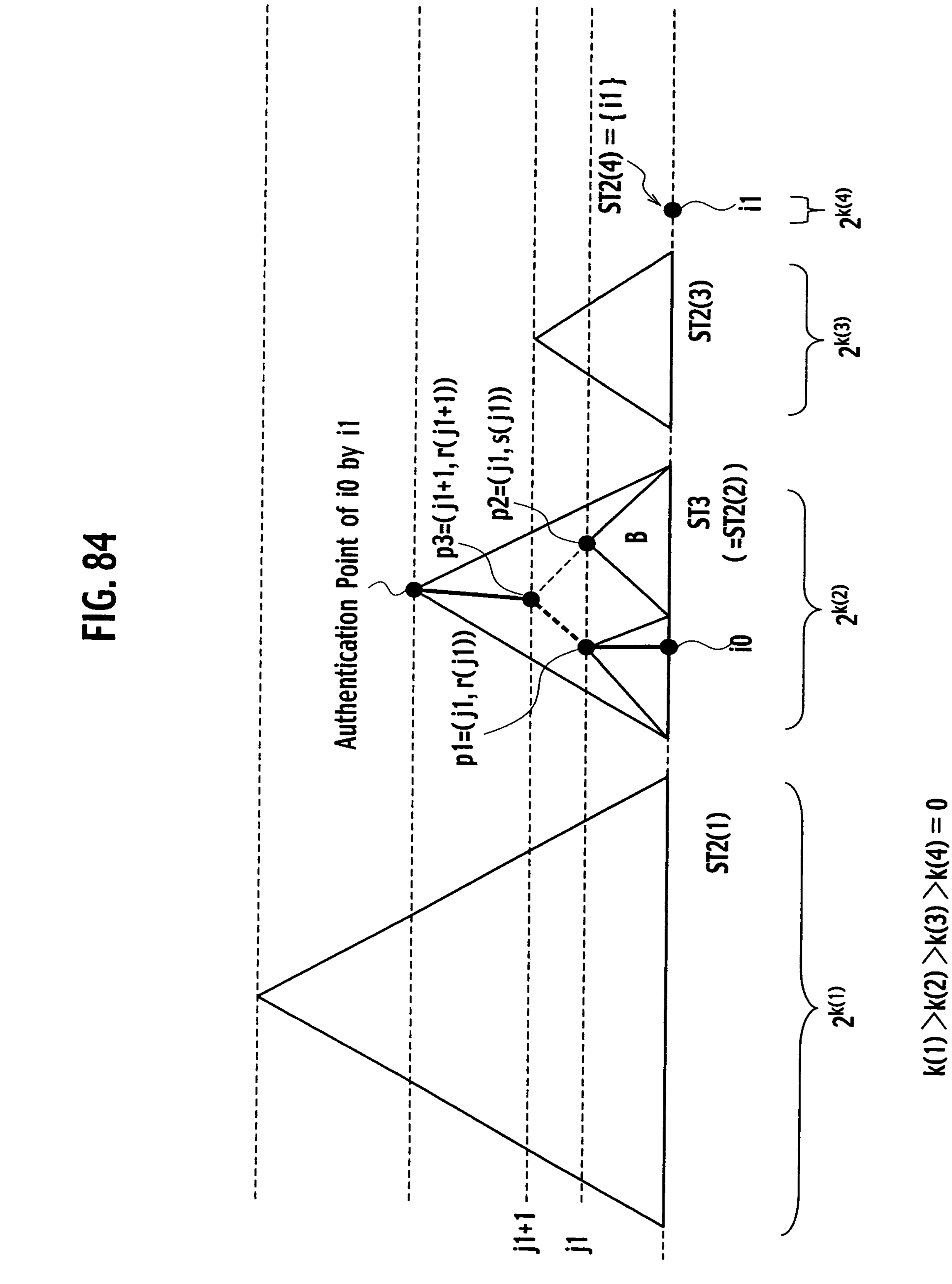
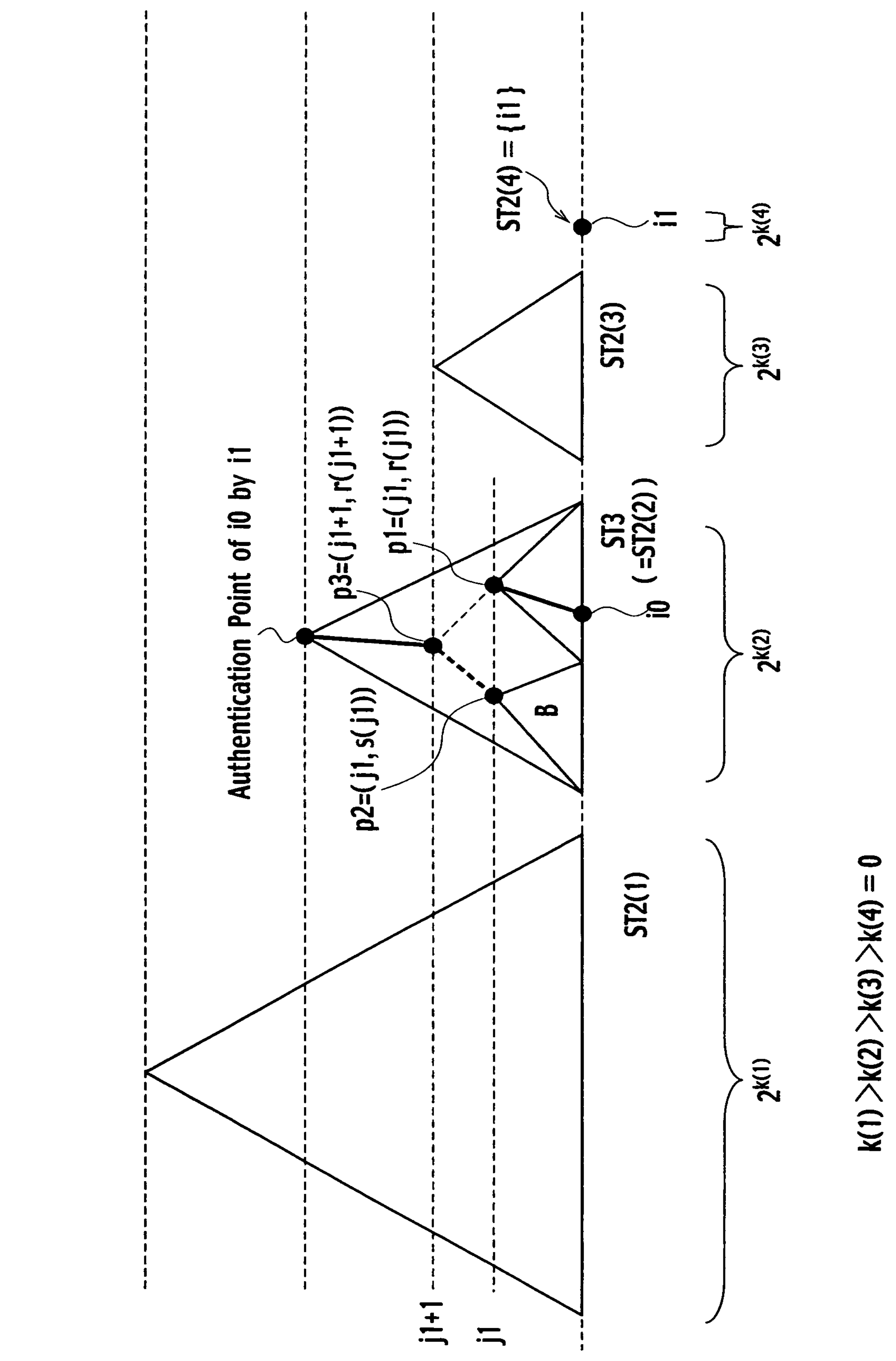

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

FIG. 84



$k(1) > k(2) > k(3) > k(4) = 0$

FIG. 85


Authentication Point of i0 by i1
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
B
ST3
(=ST2(2))
i0
ST2(1)
ST2(3)
ST2(4) = {i1}
i1
$2^{k(1)}$
$2^{k(2)}$
$2^{k(3)}$
$2^{k(4)}$
k(1) > k(2) > k(3) > k(4) = 0
j1+1
j1